

高等学校信息安全专业规划教材

信息系统安全

林果园 别玉玉 刘凯 编著

清华大学出版社

21世纪高等学校信息安全专业规划教材

信息系统安全

林果园　别玉玉　刘　凯　编著

清华大学出版社
北　京

内容简介

本书阐述信息系统规划、设计、实施过程中涉及的安全问题。基于硬件、软件、人员3个层面，在介绍相关模型和概念的基础上，探讨了信息系统安全工程中物理设备安全、环境安全需求与通信硬件安全的规划、需求和测试，分析了信息系统数据在使用中的安全性，信息系统赖以生存的软件自身的安全问题，以及使用信息系统的人员的安全管理与控制。另外，本书还对信息系统安全相关的风险评估与减缓、安全标准与规范、应急与恢复、安全技术和安全解决方案进行了必要的介绍。

本书可作为计算机、软件工程、信息安全、物联网工程等相关专业的教材，也可供信息技术人员学习参考。

图书在版编目(CIP)数据

信息系统安全/林果园等编著．—北京：清华大学出版社，2012.11
(21世纪高等学校信息安全专业规划教材)
ISBN 978-7-302-29633-1

Ⅰ．①信…　Ⅱ．①林…　Ⅲ．①信息系统－安全技术　Ⅳ．①TP309

中国版本图书馆CIP数据核字(2012)第184364号

责任编辑：魏江江　李　晔
封面设计：
责任校对：梁　毅
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：15.25　　**字　　数**：380千字
版　　次：2012年11月第1版　　**印　　次**：2012年11月第1次印刷
印　　数：1～　000
定　　价：　.00元

产品编号：043631-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

（3）实施精品战略，突出重点。规划教材建设把重点放在专业核心（基础）课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

（4）支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

（5）依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21 世纪高等学校信息安全专业规划教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

前　　言

信息系统所面临的各种安全威胁日益突出，信息安全问题已成为涉及国家政治、军事、经济和文教等诸多领域的战略安全问题。信息系统安全问题伴随着信息技术在企业、政府及社会各个角落的普及而日益突出，信息系统安全研究的重点，则伴随着网络安全隐患的不断暴露和安全知识的深化在不断调整。从经典的密码学到新兴的反黑防毒技术，再到现在的云查杀，无不渗透着这样一个道理：信息系统的安全方兴未艾、任重道远。

大量研究表明，信息系统本身就充满动态性。例如信息系统的需求是动态的，安全漏洞具有动态性，系统建设是动态的，网络拓扑也是动态的。这些动态的因素要求网络的防御也必须是动态的。信息系统的安全防护除了应采取加密、访问控制和防火墙外，还应当动态地检测和监控网络，利用相关检测工具了解和评估当前系统的安全状态，发现新的威胁和弱点，并通过循环反馈及时做出响应，将信息系统调整到“最安全”和“风险最低”的状态。

信息保障强调信息系统整个生命周期的防御和恢复，同时安全问题的出现和解决方案超越了纯技术范畴。为了确保信息系统的可用性、完整性、机密性、可控性、不可否认性等特性，仅仅靠技术是难以奏效的。所以信息安全保障要依赖于人、技术、管理三者共同完成。

本书以解决信息系统日益严重的安全问题为出发点，紧密结合信息管理、网络工程、通信工程、信息工程、信息安全等相关专业的实际需要，将抽象的信息系统安全概念、理论和方法融入到信息系统的设计、规划与管理等方面。

本书具有以下特点：

（1）将信息安全的概念、理论和技术与通用信息系统工程领域的最新成果相结合。

（2）从信息系统实际应用的角度出发，对所涉及的系统安全需求、规划与运行管理安全进行了全方位的阐述。

（3）强调基本理论和工程技术相结合，为便于学习，书中将以具体实例阐述信息系统安全的实施方案。

全书共分 9 章，每章都配有小结和习题。第 1 章为概述，主要介绍相关基本概念，如信息、信息系统、信息系统安全，并对信息系统安全研究的内容进行了阐述。第 2 章围绕信息系统安全工程 ISSE 及周期模型展开论述，引入信息系统安全工程的相关基本概念，主要介绍周期模型、ISSE 过程、ISSE 的基本功能、安全规划与控制、安全需求、

安全设计和安全运行，接着从生命周期的角度论述了安全支持和风险管理技术。第 3 章讲述信息系统安全规划，在讨论信息系统安全规划的目标、原则、作用和步骤的基础上，重点论述信息安全规划的内容，包括计算模式安全规划、信息资源安全规划、网络与系统安全规划、组织与管理安全规划，最后提出信息系统安全规划的模型和方法。第 4 章为信息系统安全需求，分别阐述不同层次、不同类别的安全需求，并对安全需求进行分析，最后介绍了信息系统各基本阶段的安全需求。第 5 章为信息系统安全设计，从安全体系结构和安全生命周期两个角度对信息系统安全设计做出分析。第 6 章讲解信息系统的安全性测试技术，在讨论测试目标、原则等基本概念之后，从硬件和软件两个层面重点阐述相关安全性测试方法。第 7 章围绕信息系统运营中的安全管理展开论述，主要讲解相关人事管理、事件管理、灾难备份与恢复和安全审计技术。第 8 章讲述了信息系统安全风险评估的有关概念和方法，主要包括评估过程、评估方法以及评估实施过程中的若干事项。第 9 章提供相关信息系统安全示例。

全书由林果园主编、统稿，其中第 1、3、5、7、9 章由别玉玉负责编写，第 2、4、6、8 章由刘凯负责编写。

在本书写作过程中，吸收了很多国内外同行关于操作系统的最新研究内容，参考了大量学术著作和研究成果，有的已经在参考文献中列出，但由于篇幅所限，恕不能一一列出，在此一并表示感谢！

由于编者水平有限，书中难免有错，殷切希望广大读者批评指正。

编　者

2011 年 4 月

目　　录

第1章　概　　述

1.1　信　　息

当今时代是一个信息化的时代，随着信息化进程的不断深化，人类社会对信息科学与信息技术的依赖与日俱增，一位美国科学家曾说过："没有物质的世界是虚无的世界，没有能源的世界是死寂的世界，没有信息的世界是混乱的世界。"由此可见信息的重要性，同时也说明信息本身是有秩序、有价值的。

自然界的万事万物无时无刻不在传递着信息。"今天天气很好，秋高气爽，青草慢慢转黄，湖中的睡莲随风吐露芬芳……"，仅从这一句话我们就能得到丰富的信息，天气情况是一种信息，色彩是一种信息，芳香也是一种信息。

1.1.1　信息的含义

信息是信息论中的术语，常常指消息中有意义的内容。信息的概念由来已久，最早可以追溯到两千多年前的西汉，作为消息理解，但当时对信息的使用仅限于日常用语。随着人类社会文明程度的不断提高，人们对信息的认识也在不断提高和深入，但至今对信息还没有一个公认的定义。

1928年美国数学家哈特莱(Hartley)在《信息传输》中首先提出：信息的具体形式是由代码、符号组成的消息，并用选择的自由度来度量信息的大小。他在文中指出消息是信息的载体，信息是包含在消息中的抽象量，从而在概念上对消息和信息加以区分。哈特莱认为"信息是选择的自由度"。

1948年，美国数学家、信息论的创始人香农(Shannon)在《通信的数学理论》中指出："信息是用来消除事物不确定性的东西"。香农创立的信息论为人们开启了探索信息时代奥秘的大门。

同一年，美国著名数学家、控制论的创始人维纳(Wiener)在《控制论》一书中指出"信息就是信息，既非物质，也非能量"。

上述著名学者关于信息的定义在某种程度上描述了信息的一些特征，但是还不够全面，除此之外，关于信息的定义，国内外还有很多种不同的理解和说法，例如：

(1) 信息是物质、能量及其属性的标识。

(2) 信息是事物现象及其属性标识的集合。

(3) 信息是确定性的增加。

(4) 信息是独立于物质和能量之外存在于客观世界的第三要素。

(5) 信息是系统的组成部分，是物质和能量的形态结构、属性和含义的表征，是人类认识客观的纽带。

目前对信息的描述也是众说纷纭，但实质内容并没有太大差别，主要区别在于概括问题的层次不同。中国人工智能学会理事长钟义信教授认为信息的概念是有层次的，他根据“本体论”和“认识论”两个最重要的层次，对信息做出定义。所谓“本体论”层次，即为无约束条件层次，信息可定义为事物运动的状态及状态改变的方式。这里的“事物”泛指存在于人类社会、思维活动和自然界中一切可能的对象。在该层次上定义的信息是广义的信息，其使用范围也最广。而“认识论”层次是受主体约束的层次，在主观认识论层次上，信息是认识主体所感知的或所表述的相应事物的运动状态及其改变的方式。其中主体所感知的是外部世界向主体输入的信息，主体所表述的则是主体向外部世界输出的信息。

1.1.2 信息的性质

信息本身虽然很抽象，它既不是物质也不是能量，却又与物质和能量有相互依赖的关系。信息的本质属性——物质性决定了它的一般属性，主要包括普遍存在性、客观性、层次性、无限性、有序性、相对性、共享性、价值性、时效性等。

(1) 普遍存在性。信息的“本体论”定义是事物的运动状态及其改变方式，事物的存在具有普遍性，并且事物的状态无时无刻不在发生着运动变化，因此信息也具有普遍存在性。

(2) 客观性。信息是客观存在的，不以人的意志为转移。信息的客观性表现为信息是客观事物发出的信息，信息以客观事实为依据。

(3) 层次性。信息是分等级的，根据对信息的约束条件的不同，可以将信息划分为不同的层次，“本体论”和“认识论”是划分信息的两个最基本最重要的层次。随着对信息约束条件的增加，信息的层次越低，应用范围也越窄。

(4) 无限性。物质的无限性以及事物运动状态的不断变化决定了信息的无限性。因此也出现了“信息爆炸”的问题，汹涌而来的信息有时使人无所适从，从浩如烟海的信息海洋中迅速而准确地获取自己最需要的信息，变得非常困难。

(5) 有序性。“没有信息的世界是混乱的世界”、“信息是消除事物不确定性的东西”，这些都说明了信息可以增加事物的有序性。信息的这一性质具有非常重要的价值，要想使事物变得有序，必须从外界获取信息。

(6) 相对性。由于人们认识事物的能力存在着一定的差异，对于同一事物，不同的观察者获取的信息量可能不同；对于相同的信息，不同的人的理解也存在差异性，因此信息是相对的。

(7) 共享性。萧伯纳对信息的共享性有一个形象的比喻：你有一个苹果，我有一个苹果，彼此交换一下，我们仍然是各有一个苹果。如果你有一种思想，我也有一种思想，我们相互交流，我们就都有了两种思想，甚至更多。这个例子说明了信息不会像物质一样因为共享而减少，反而可以因为共享而衍生出更多。信息的共享性对人类社会的发展和进步具有举足轻重的意义。

(8) 价值性。信息是一种资源，信息经过加工可以对人类的生产生活产生重大影响，信息可以转换为物质、能力、资金、人力和时间。因此，信息是具有价值的资源。

(9) 时效性。事物状态的不断变化决定了信息的动态性，信息一旦不能反映事物的最新变化就会失去其本身的价值，所以说信息是有“寿命”的。一条信息在某一时刻价值非常高，但过了这一时刻，可能一点价值也没有。例如，战争时期敌方的信息在某一时刻具有非

常重要的价值，可以决定一场战争或战役的胜败，但过了这一时刻，这一信息就变得毫无意义。所以说信息具有非常强的时效性。

现实生活中的各种实例能够帮助人们更透彻地理解信息的上述性质，从而更深入地了解信息的本质。在信息化程度不断提高的社会中，信息的作用越来越不容小觑。信息是比物质和能量更有价值的资源，全面理解信息的概念和性质，可以帮助人们准确有效地利用信息为人类创造更多的财富。

1.2　信息系统

信息是数据所表达的客观事实，而信息系统则是对这种数据所表达的客观事实即信息进行采集、加工处理、存储和传输，并能向有关人员提供有用信息的系统。因此，信息系统是以信息为基础为人类提供服务的工具。

1.2.1　系统的概念

“系统”一词源于古希腊语，是部分组成整体的意思，系统的思想更是源远流长，早在 1937 年，系统论的创始人 L. V. 贝塔朗菲(L. V. Bertalanffy)就提出了一般系统论原理，他将系统定义为“相互作用的诸要素的复合体”。随着系统论的不断发展，有学者提出系统是由一些相互联系、相互制约的若干组成部分结合而成的、具有特定功能的一个有机整体。尽管系统一词频繁出现在社会生活和学术领域中，但长期以来，系统的概念及描述尚无统一规范的定论。

我们一般将系统定义为由若干要素以一定结构形式联结构成的具有某种功能的有机整体，可以从 3 个方面进行理解。首先，系统由若干要素组成。这些要素可能是一些个体、元件、零件，也可能其本身就是一个系统(或称为子系统)。如运算器、控制器、存储器、输入输出设备组成了计算机的硬件系统，而硬件系统又是计算机系统的一个子系统。其次，系统具有一定的结构。一个系统是其构成要素的集合，这些要素相互联系、相互制约。系统内部各要素之间相对稳定的联系方式、组织秩序及控制关系的内在表现形式，就是系统的结构。例如，钟表是由齿轮、发条、指针等零部件按一定的方式装配而成的，但一堆齿轮、发条、指针随意放在一起却不能构成钟表；人体由各个器官组成，多个器官的简单拼凑并不能成为一个有行为能力的人。最后，系统具有一定的功能，或者说系统要有一定的目的性。系统的功能是指系统与外部环境相互联系和相互作用中表现出来的性质、能力和功能。例如信息系统的功能是进行信息的收集、传递、储存、加工、维护和使用，辅助决策者进行决策，帮助企业实现其目标等。

从宏观角度，系统可分为自然系统、人工系统和复合系统。

(1) 自然系统：系统内的个体按自然法则存在或演变，产生或形成一种群体的自然现象与特征。自然系统包括生态平衡系统、生命机体系统、天体系统、物质微观结构系统以及社会系统等。

(2) 人工系统：系统内的个体根据人为的、预先编排好的规则或计划好的方向运作，以实现或完成系统内各个体不能单独实现的功能、性能与结果。人工系统包括立体成像系统、

生产系统、交通系统、电力系统、计算机系统、教育系统、医疗系统、企业管理系统等。

(3) 复合系统：复合系统是自然系统和人工系统的组合。复合系统包括导航系统、交通管理系统、人机系统等。

1.2.2 信息系统的概念

信息系统是由计算机软硬件、网络通信设备、数据资源以及人组成的以收集、处理、存储及传输信息为目的的人机一体化系统。任何一种信息系统都由信源、信道和信宿组成(如图1.1所示)。过去的信息系统并不涉及计算机相关设备与技术，但是随着网络通信技术与计算机技术的飞速发展，现代信息系统基本上都离不开通信技术和计算机的支持，并且在很大程度上提高了信息系统的处理能力和使用效率。

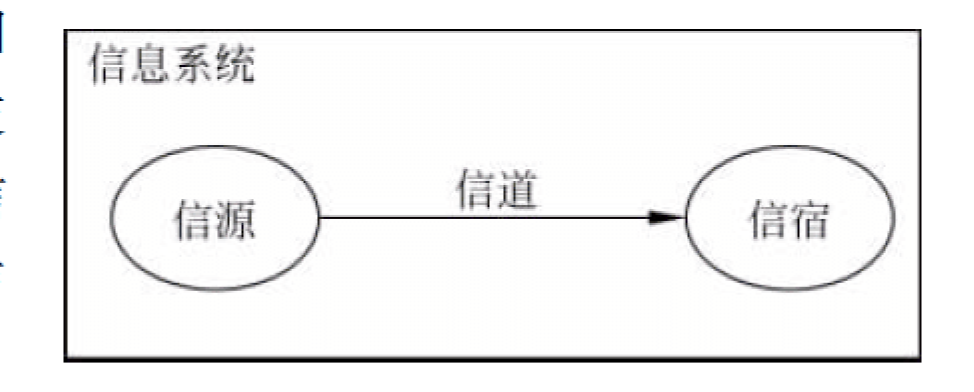


图1.1 信息系统的结构图

从信息系统的发展和系统特点来看可以将信息系统分为以下几种类型：

1. 管理信息系统(Management Information System，MIS)

管理信息系统是一个以人为主导，面向管理工作，以提高信息管理效率和收益为目的的人机一体化系统。管理信息系统利用计算机相关设备进行数据信息的处理，并为用户提供管理所需要的各种信息，同时支持企业高层决策、中层控制和基层操作。

2. 办公自动化系统(Office Automation System，OAS)

针对手工办公方式低效、复杂的缺点，办公自动化系统利用Internet/Intranet技术，基于工作流的概念，用各种现代化的办公设备代替人来完成办公业务活动，使企业内部人员可以方便快捷地共享信息，高效地协同工作，实现迅速、全方位的信息采集与处理，并支持企业科学管理与决策。

3. 决策支持系统(Decision Support System，DSS)

决策支持系统是管理信息系统进一步发展的产物，通过数据分析、建立模型、模拟决策过程和方案等手段，并调用多种分析工具和信息资源，来辅助决策者做出高水平以及高质量的决策。

4. 数据处理系统(Data Processing System，DPS)

数据处理系统能够将输入的数据信息通过加工、整理、分析并计算转换成易于被人们接受的信息形式，并将处理后的信息进行有序存储，随时通过外部设备输出给用户。

1.2.3 信息系统的发展

随着人类社会的发展变化，作为人类的重要服务工具的信息系统也在持续不断地发展变化。计算机技术、通信技术和管理科学的发展是信息系统发展的原始动力。虽然在人类文明起源阶段信息系统和信息处理就已经存在了，但是直到电子计算机的问世、信息技术的飞跃以及现代社会对信息需求量的剧增，信息系统才飞速发展起来。

信息系统的发展具有阶段性，描述其发展进程的是阶段论，具有代表性的模型是诺兰模型、西诺特模型和米切模型。

1. 诺兰模型

通过对 200 多个公司和部门发展信息系统实践和经验的调查与总结，美国哈佛大学教授理查德·诺兰(R. Nolan)提出了著名的信息系统发展的阶段模型，即诺兰模型。诺兰认为，手工信息系统向计算机信息系统发展过程中存在一条客观的发展规律。诺兰在模型中指出，信息系统的发展经历了初始期、普及期、控制期、整合期、数据管理期和成熟期 6 个阶段(如图 1.2 所示)。

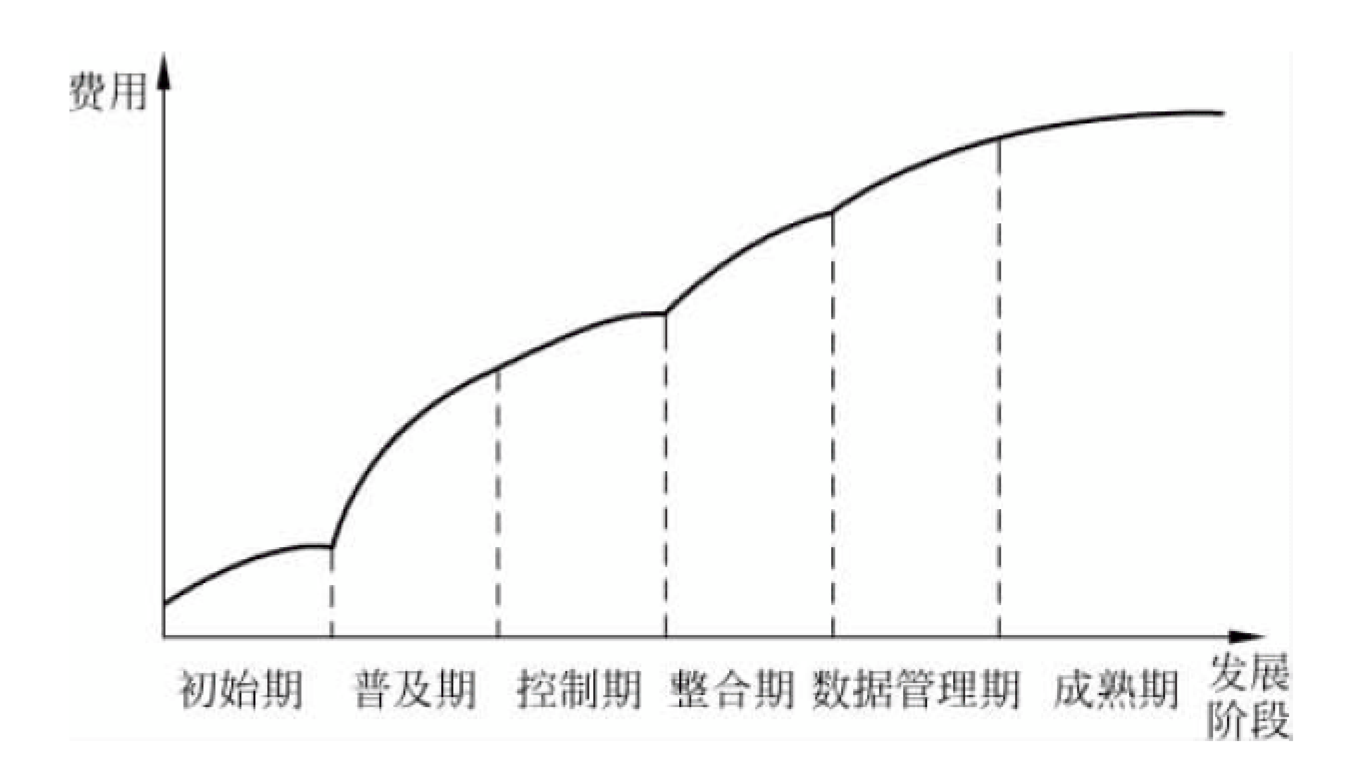


图 1.2 诺兰模型

1）初始期

在初始期，计算机刚开始用于信息处理，此时，人们对计算机的应用缺乏了解，计算机并不能得到充分的利用，仅仅用于管理财务和工资等工作。此外，缺少具备计算机操作能力的 IT 人员，计算机得不到普遍的应用。

2）普及期

随着计算机应用的不断深入，人们对计算机的兴趣越来越广泛，开始使用计算机处理大量的数据信息。随着应用需求的增加，计算机软件开发以及设备购买的投入大幅增长。在普及期，由于计算机软硬件技术的限制，同时缺乏合理的规划，往往出现盲目开发软件和盲目购买计算机设备的情况，计算机的实际应用效率并不高。

3）控制期

由于控制信息处理费用的需要，管理者召集来自不同部门的用户组成委员会，以共同规划信息系统的发展。管理信息系统成为一个正式部门，以控制其内部活动，启动了项目管理计划和系统发展方法。目前的应用开始走向正规，并为将来的信息系统发展打下基础。

4）整合期

在这一时期，从管理计算机转向管理信息资源，这是一个质的飞跃。从第一阶段到第三阶段，通常产生很多独立的实体。在第四阶段，开始使用数据库和远程通信技术，努力整合现有的信息系统。

5）数据管理期

信息系统开始从支持单项应用发展到逻辑数据库支持下的综合应用。开始全面考察和评估信息系统建设的各种成本和效益，全面分析和解决信息系统投资中各个领域的平衡与协调问题。

6）成熟期

信息系统受到更广泛的关注和重视。正式的信息资源计划和控制系统投入使用，以确保管理信息系统支持业务计划。信息资源管理的效用充分体现出来。

诺兰模型的作用在于衡量信息系统当前所处的状态，有利于选择系统开发的时机，同时帮助人们对系统的规划做出合理的安排，控制系统的发展方向。

2. 西诺特模型

1988年，西诺特（W. R. Synnott）参照“诺兰模型”提出了一个新的模型，这是一个过渡性的理论，主要考虑到信息随时代变迁的变量。他用4个阶段的推移来描述计算机所处理的信息。从计算机处理原始数据的“数据”阶段开始，逐步过渡到用计算机加工数据并将它们存储到数据库的“信息”阶段；接着，经过诺兰所说的“技术性断点”，到达把信息当做经营资源的“信息资源”阶段；最后到达将信息作为带来组织竞争优势的武器，即“信息武器”阶段。当前，发达国家都接受了西诺特对诺兰模型的改善。

3. 米切模型

20世纪90年代，美国的信息化专家米切（Mischel）对诺兰模型进行了修正，提出了米切模型，揭示了信息系统整合与数据管理密不可分的内在联系，认为系统整合期的重要特征就是做好数据组织，也可以说信息系统整合的本质是数据整合或集成。

米切的信息系统发展阶段论把综合信息技术应用持续发展，按照若干特征概括为4个阶段，即起步阶段、增长阶段、成熟阶段和更新阶段。该模型的特征不仅仅是在数据处理工作的增长和管理标准化建设方面，而且要涉及有关知识、理念、信息技术的综合水平及其在企业经营管理中的作用和地位。决定这些阶段的特征的是技术状况、代表性应用和集成程度、数据库存取能力、信息技术融入企业文化程度以及全员素质、态度和信息技术视野等，米切模型如图1.3所示。

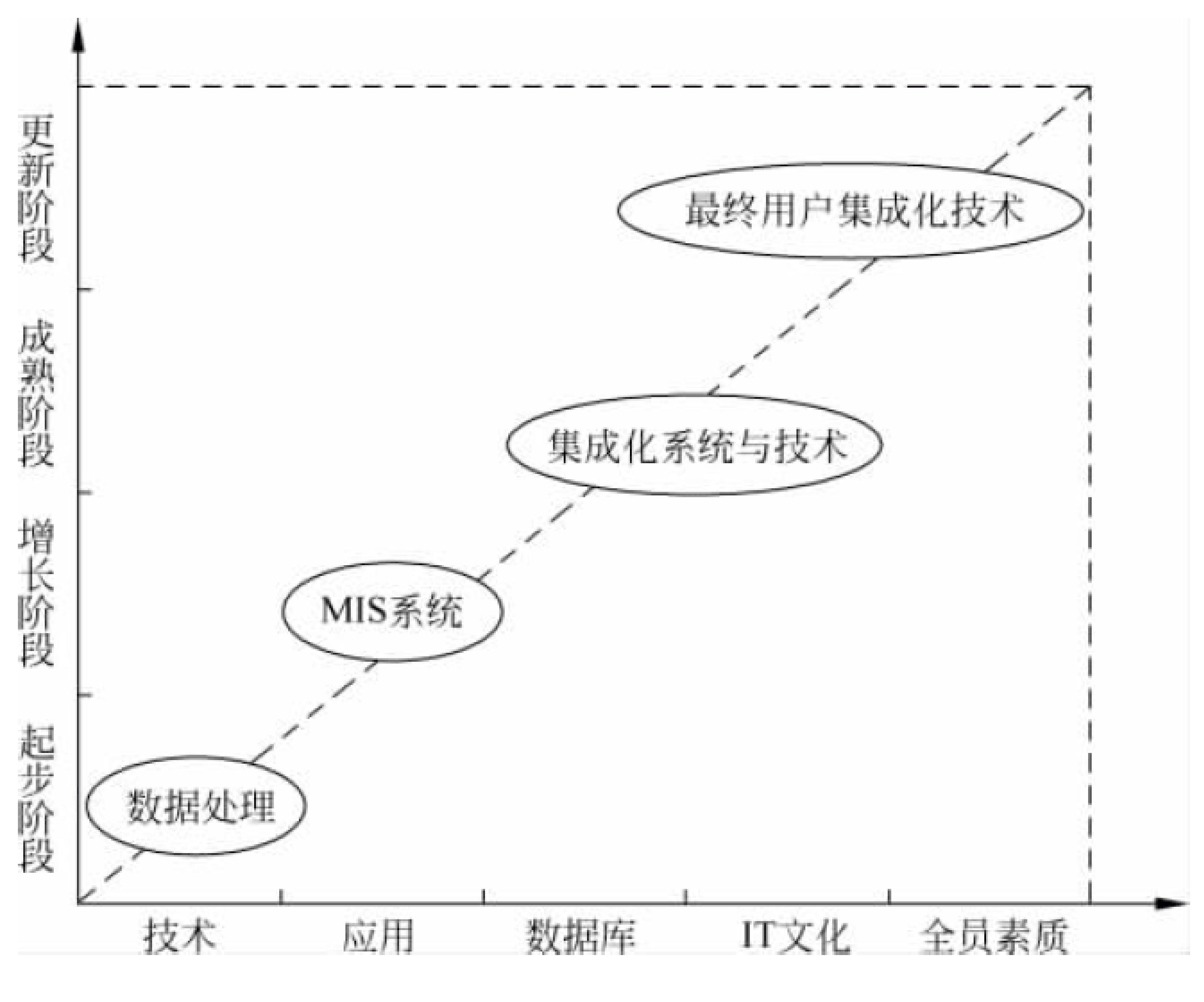


图 1.3 米切模型

米切模型可以帮助企业了解自身 IT 综合应用在现代信息系统的发展阶段中所处的位置，发现在综合信息技术应用连续发展方面的差距，并找到改进方向，采取合理的措施。

4. 其他代表性观点

从信息处理功能和内容来看，信息系统大致经过了 4 个发展阶段：单项事务处理、系统处理、决策支持和综合集成。这 4 个阶段反映了计算机辅助管理和业务活动由初级到高级的发展过程，又显示了信息活动在不同层次与深度上对管理业务活动的支持。信息系统发展的这 4 个阶段的核心技术、主要功能、系统目标以及代表性系统如表 1.1 所示。

表 1.1　信息系统发展的 4 个阶段

阶段	时间	核心技术	主要功能	系统目标	代表性系统
单项事务处理阶段	1950—1970 年	高级语言程序设计、文件管理	文字处理、制表、统计、计算	提高文书、统计以及计算等事务处理的工作效率	电子数据处理系统
系统处理阶段	1960—1980 年	计算机网络、通信、数据库技术	计划、综合统计、管理报告生成、计算机辅助设计与制造	提高管理信息处理的综合性、系统性、准确性和及时性	传统的 MIS、CAD 系统、CAM 系统
决策支持阶段	1970—1990 年	人机对话、模型管理、人工智能的应用	分析、优化、评价、预测	为组织决策者在决策过程中的活动提供决策支持，以改善决策有效性	决策支持系统、计算机集成制造系统
综合集成阶段	1990 年以来	数据挖掘、智能代理、高速信息传输及多媒体信息处理技术	综合集成上述功能，尤其对人的智能活动提供主动支持	实现信息的集成管理和综合服务，促进制度创新和业务流程改造，提高人员素质，创造良好的工作环境	互联网、Web 服务、虚拟企业管理系统、协作商务

信息系统发展的终极目标是任何人在任何时间地点，任何情况下都能安全、方便并且廉价地获取、利用信息。但遗憾的是，这是一个不可能达到的极限，只能尽可能地趋近。

1.2.4　信息系统的功能

信息系统是以加工处理信息为主要目的的系统。1.1 节已经对信息给出了诸多解释。认识论中的信息是不确定度的减少或传递中的知识差，哲学界把信息与有序度联系起来，因此，信息是以传递知识差的形式来减少不确定度、增加系统有序性的资源。从这一点来看，信息系统就是减少不确定性的工具。信息系统作为一种与信息有关的工具，理应具备以下基本功能：信息的输入、信息的处理、信息的存储、信息的输出和信息的控制。

1. 信息的输入功能

输入功能取决于信息系统所要达到的目标及信息环境和系统能力的许可。

2. 信息的处理功能

要想使输入的原始数据变成对企业或用户有用的信息，就必须对信息进行综合加工处理。信息处理一般包括真伪辨别、分类整理、排错校验和加工分析 4 个环节，处理方式有分

类、查询、排序、统计、预测、结算、模拟等，通常使用的数据处理工具有数据挖掘技术和基于数据仓库技术的联机分析处理。

3. 信息的存储功能

信息输入系统以后，经过加工处理形成有用信息。由于不同信息的属性、价值和时效不同。因此，必须将这些处理后的信息进行存储保管，以便随时调用。当所需存储的信息量非常庞大时，就要依靠先进的信息存储技术，来提高信息的存储能力。系统存储各种信息数据和资料的能力称为存储功能，包括物理存储和逻辑存储两种形式，物理存储是将信息存储在适当的物理介质上，而逻辑存储是按照信息的内在联系将其组织成一定的结构来存储和使用。

4. 信息的输出功能

信息系统的各种功能都是为了保证最终实现最佳的输出功能。衡量信息系统的有效性关键不在于信息的输入、处理、存储等环节，而在于信息输出的实效、精度和数量能否充分满足信息系统的用户需求。信息的输出还要根据信息的特点，选择合适的输出媒体、输出格式、输出方式，以保证信息传递便捷准确、使用方便以及满足保密需要等。

5. 信息的控制功能

对构成系统的各种信息处理设备进行控制和管理，对整个信息加工、处理、传输、输出等环节通过各种程序进行控制，保证系统安全、有序地运行。

1.3 信息系统安全

信息系统是企业和国家的宝贵资源，也是竞争对手和敌对势力攻击的对象。随着互联网的迅速发展，网络安全形势也愈加严峻，病毒、木马等恶意程序以爆发式的形态增长，泛滥于整个互联网领域。信息系统的安全性也成为全球性的社会问题，是当前信息系统建设的重中之重。

1.3.1 信息系统安全的概念

安全是相对威胁来说的，或者说，安全是使系统免于威胁的一种状态。有人直接将其解释为“客观上不存在威胁，主观上不存在恐惧”。反过来说，如果“客观上存在威胁，主观上存在恐惧”就是不安全的。因此，信息系统安全即是一种系统客观上不存在威胁，用户主观上不存在恐惧的安全状态。信息系统安全学科就是研究如何应对各种威胁保障系统安全性的一门科学。

信息系统安全目前还没有一个权威、公认的解释和标准的定义，一个基本的理由就是信息系统安全的概念是随着信息系统的发展，随着信息系统在社会生活中的地位的变化，随着人们对信息系统安全的重视和理解不断深化的。

1994年，我国国务院发布了《中华人民共和国计算机信息系统安全保护条例》。根据该条例，信息系统安全是指：“保障计算机及其相关的和配套的设备、设施（含网络）的安全以及运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统

的安全运行。”

一般来说，多数人倾向于把信息系统安全的概念分为 3 个层次：通信保密(Communication Security)、信息防护(Information Protection)和信息保障(Information Assurance)。

1. 基于通信保密的信息系统安全

信息保密的基本技术是加密，目的是控制信息共享的范围，保障信息传递过程中的机密性。密码技术最早因战争中的情报传递而诞生，并在军事和市场竞争以及外交活动的推动下，在加密与解密之间的相互博弈中不断发展。早期的信息保密技术中比较著名的是公元一世纪，凯撒(Caesar)大帝使用过的单字母替代密码，称为 Caesar 密码，是最早的换位密码。之后又有很多人对密码技术做出很大贡献，值得一提的是 19 世纪德国发明家亚瑟发明了加密机器 Enigma，该加密机是当时最可靠的加密系统，将人类从手工编写密码的繁重劳动中解放出来。直到计算机出现之前，密码学一直是通信领域研究的课题。计算机的出现及其发展大大提高了运算能力，计算机时代的信息保密随之而来，开始出现了对称密钥体系和不对称密钥体系。

2. 基于信息系统防护的信息系统安全

信息安全是在机密性的基础上，把信息安全的内涵扩充到完整性、可用性、真实性和可控性。它是一种被动的防御思想，所以也称为信息(系统)防护，具体目标是：

- 系统保护——对设施和技术系统可靠性、完整性和可用性的保护。
- 信息内容保护——保护系统中数据的机密性、完整性和可用性。

信息安全的被动防御还体现在这些概念是从教训中总结出来的，也是在计算机诞生后的信息处理实践中完善起来的。这个概念的形成经历了计算机安全、计算机网络安全两个阶段。

3. 基于信息保障的信息系统安全

信息保障的思想是在 1995 年美国国防部提出的 PDR(Protection-Detection-Response，防护—检测—响应)模型中体现出来的，信息保障的概念也是在 PDR 模型的不断完善中发展的。随着主动防御思想的深入发展，信息系统安全的研究也从不惜一切代价把入侵者阻挡在系统之外的被动防御，开始转变为强调信息系统在受到攻击的情况下稳定运行能力。1998 年，美国国家安全局在其研究成果《信息保障技术框架》中提出了基于 PDR 的 PDRR (Protect-Detect-React-Restore)主动防御模型。PDRR 是一种运用“纵深防卫策略”的模型，它在防卫、检测、响应之后又增加了恢复功能，恢复是指使系统具有很快的恢复能力。一个系统能够在受到攻击以后，迅速地恢复工作能力，或者不损失工作能力，就很好地避免了处于被动挨打的境地。信息系统在面临各种威胁与攻击时，有两种选择：攻击发生前做出调整或攻击发生后进行再调整。可见，基于主动防御的信息系统保障思想对我们的社会是多么重要。

大量研究发现，信息系统本身就充满动态性。例如，信息系统的需求是动态的，安全漏洞具有动态性，系统建设是动态的，网络拓扑也是动态的。这些动态的因素要求网络的防御也必须是动态的。信息系统的安全防护除了应采取加密、访问控制和防火墙外，还应当动态地检测和监控网络，利用相关检测攻击了解和评估当前系统的安全状态，发现新的威胁和弱点，并通过循环反馈及时做出响应，将信息系统调整到“最安全”和“风险最低”的状态。

信息保障强调信息系统整个生命周期的防御和恢复，同时安全问题的出现和解决方案超越了纯技术范畴。为了确保信息系统的可用性、完整性、机密性、可控性、不可否认性等特性，仅仅靠技术是难以奏效的。所以信息安全保障要依赖于人、技术、管理三者共同完成。

本书中将信息系统安全定义为：确保以电磁信号为主要形式的，在计算机网络化(开放互联)系统中进行自动通信、处理和利用的信息内容，在各个物理位置、逻辑区域、存储和传输介质中，处于动态和静态过程中的机密性、完整性、可用性、可审查性和抗抵赖性，与人、网络、环境有关的技术安全、结构安全和管理安全的总和。其中人指的是信息系统的主体，包括各类用户、支持人员以及技术管理和行政管理人员；网络是指计算机、网络互连设备、传输介质、信息内容及其操作系统、通信协议和应用程序所构成的物理的与逻辑的完整体系；环境指系统稳定和可靠运行所需要的保障体系，包括建筑物、机房、动力保障与备份以及应急与恢复体系。

从系统过程与控制角度讲，信息系统安全就是信息在存取、处理、集散和传输中保持其机密性、完整性、可用性、可审计性和抗抵赖性的系统辨识、控制、策略和过程。"系统辨识"主要研究系统数学模型的建立、模型类型的确定、高精度参数的估计方法等。"控制"是指信息系统能够根据变化进行调整，调整的方向和目标是保持风险处于可接受范围，并且逐步降至最低，从而保持系统动态平衡的状态。针对信息系统所面临的各种威胁及系统脆弱性，通过风险分析，确定安全目标和安全等级，进而建立安全模型，提出控制"策略"，并对信息系统安全进行评估，制定安全保障和安全仲裁等对策。"过程"指信息系统状态的变化在空间上的延伸和时间上的持续。过程和状态不可分割，两者相互依存、相互作用和相互制约。

上述定义源于两种研究方法：一是将信息系统的安全作为状态来研究；二是将信息系统的安全作为对状态的控制调节来研究，控制调节的目的是使系统安全稳定在某一可控的特定状态内。

1.3.2 信息系统安全研究的内容

信息系统安全问题伴随着信息技术在企业、政府及社会各个角落的普及而日益突出，信息系统安全研究的重点，则伴随着网络安全隐患的不断暴露和安全知识的深化在不断调整。从经典的密码学到新兴的反黑防毒技术，无不渗透着这样一个道理：信息系统的安全方兴未艾、任重道远。下面针对当前信息系统安全研究的主要内容和领域做出总结，对几大研究热点分别予以剖析。

导致信息系统的不安全因素包括以下几种：

(1) 网络的开放性。网络支持信息共享，所以其最大的特点是对外开放，而用户众多、良莠不齐，从而导致误用、滥用甚至恶意破坏的情况发生。

(2) 信息系统本身存在着脆弱性。黑客或恶意破坏者会利用系统不规范的安全配置或者错误的配置打开入侵系统的缺口。用户的误操作或不恰当使用会造成不安全的后果甚至会导致系统崩溃。网络传输协议自身的弱点容易造成信息泄密。

(3) 管理者不重视系统的安全管理。即使有了很详细的安全解决方案，但如果管理混乱、技术粗糙，不及时更新、修补旧的漏洞等，就会使得安全解决方案形同虚设。

事实表明，绝大多数信息系统发生的不安全事件都可以从上述几点因素中找出原因。因此，努力寻找解决这些不安全因素的方法，提高安全管理水平成为目前信息系统安全研究的热点。具体来说，包括如下几个方面：

(1) 安全体系结构与技术的研究。

安全体系结构理论主要研究如何利用形式化的数学描述和分析方法建立信息系统的安全体系结构模型。

(2) 安全协议理论与技术的研究。

众所周知，TCP/IP 协议以及基于 TCP/IP 的 HTTP、FTP 等都存在着不安全的问题。因此致力于提高、改进这些协议的安全性甚至创新的安全协议始终是人们追求的目标。目前，安全协议理论和技术的研究主要包括协议的安全性分析方法和各种实用安全协议的设计与分析。

协议的安全性分析方法主要有两类：一类是攻击检验法，通过使用各种有效攻击方法，逐一对使用安全协议的系统进行攻击，以检验安全协议抵抗攻击的能力，这种分析方法的难点在于攻击方法的设计和选择；另一类是形式化分析方法，即采用各种形式化的语言或者模型，建立安全协议模型，并按照规定的假设和分析、验证方法等来证明协议的安全性。目前形式化分析方法是安全协议研究中的热点之一，但是就其实用性来说，还没有什么突破性的进展，主要原因是协议安全性的形式化过程比较困难。

安全性协议的形式化分析方法可以概括为如下几个研究思路：

- 基于推理知识和信任的模态逻辑来建立所分析协议的安全需求模型。
- 基于状态搜索工具和定理证明技术证明协议的正确性。
- 设计专门的专家系统来制定协议的校验方案并进行协议检验。
- 基于密码学系统的代数特性开发协议的形式化模型。

抛开复杂的形式化分析方法不说，许多实用协议已经作为安全性协议获得了实际应用。虽然在理论上证明它们的安全性还有很长的路要走，但是实际应用效果却不差。实用安全协议的安全性分析特别是 PKI、IPSec、TLS 等是当前协议研究中的热点。

(3) 信息系统安全监控与保护技术的研究。

信息系统安全监控和保护技术可以说是目前安全研究中与实际结合最紧密的一个领域，也是一个热点领域。因为其研究成果可以立即与实际网络产品结合而产生经济效益，所以相关组织和企业会不遗余力地投入。在此领域的研究主要包括安全整体解决方案的分析与设计、安全产品的研发等。

信息系统安全监控是为了保障系统免受外来干扰和破坏而对其实施的安全保护措施。黑客入侵手段分析、信息伪装与隐写理论和技术、信息分析与监控、入侵检测原理与报警技术、系统脆弱性扫描检测技术、应急恢复系统、计算机病毒防范等都属于网络安全监控技术的范畴。其中部分研究成果已经成为众多安全工具软件的基础。

网络保护技术主要是指网络访问控制和审计管理技术，包括防火墙、路由器、代理服务器、访问日志等。网络保护技术的特点是由硬件结合软件实现。

(4) 密码学及密码技术的研究。

密码学是研究数据加解密算法的一门科学。密码学及密码技术是保障信息系统安全最基本的技术手段。

当前密码技术研究可以分为两大趋势，其中基于数学计算的传统密码学和密码技术仍是主流。传统的密码学与密码技术基于数学计算理论，从原理上可分为经典密码算法、对称密码算法和非对称密码算法。密码学是认证技术的理论基础。认证理论和数字签名技术从20世纪80年代后期起取得了长足的发展，仍然是当前研究热点之一。数字签名和身份认证都有自己的研究体系，形成了各自的理论框架。目前数字签名的研究内容非常丰富，包括普通签名和特殊签名。在身份认证的研究中，最令人瞩目的认证方案有两类：一类是1984年Shamir提出的基于身份的识别方案，另一类是1986年Fiat等人提出的零知识身份识别方案。随后人们在这两类方案的基础上又提出了一系列实用的身份识别方案。目前人们所关注的是身份认证方案与具体应用环境的有机结合。

但是，随着计算机运算速度和生物识别理论的进步，各种基于非数学计算的密码技术相继出现，如量子密码、混沌理论、DNA密码以及基于特征识别的指纹、视网膜、虹膜、面部特征与语音特征识别技术等。

(5) 信息系统安全风险评估的研究。

信息系统安全风险评估是风险评估理论在计算机信息系统安全领域的延伸。风险评估是信息系统安全保证的关键技术，主要研究内容包括信息系统安全风险评估的理论框架和标准，以及模型、技术和方法等。

1.3.3　信息安全与信息系统安全

信息安全泛指一切以电信号、磁信号、语音等为载体的信息在输入、输出、分类、检索、排序、传输和共享中的安全，一般也包括以磁介质、纸介质、无线信道及有线信道为媒体的信息。信息系统安全指的是信息系统的安全，而非信息的系统安全。就一般意义上讲，信息安全与信息系统安全是包含与被包含的关系，信息系统安全是信息安全的一部分，信息安全具有更普遍、更广泛的含义。

信息安全问题和信息系统安全问题是信息化初期常常争论的两个热点，也是常常被混淆的概念。信息安全涉及信息的采集、传输、保管、访问的全过程，信息安全问题是指一个组织中不当的信息传递和非法使用。信息系统是由计算机及其相关的和配套的设备、设施构成的，按照一定的应用目标和规划实现对信息进行采集、加工、存储、检索等功能的系统。信息系统安全问题是信息在信息系统中传输、保管过程中可能存在的各种被非法访问的问题集合，例如，未设置防火墙可能导致的黑客入侵，未关闭可能遭受攻击的访问端口，未设置数据备份策略，系统管理员权限未经过划分等。总的来说，信息系统安全问题源自于未采取恰当的安全防护技术，以及对信息系统的管理存在隐患。

根据信息安全问题的定义，信息系统安全问题主要集中在信息通过信息系统进行传导和保管的过程中，只是信息安全问题的中间环节，信息系统安全管理措施，主要是围绕信息系统本身，而信息安全问题则涵盖了信息从采集到访问的全过程，信息安全的管理问题包括了对信息的使用者和信息系统的操作者的管理。由于信息的使用主体是人，信息系统则是生产工具，最终使用和管理的主体也是人，因此，承担信息安全问题的主体是：采集、使用信息的全体员工，包括信息系统的全部用户和系统管理人员。

1.4　本章小结

信息、材料和能源是人类社会赖以生存和发展的基础，在现代信息化社会里，我们的一切活动都离不开对信息的获取和处理，信息作为一种无形资产已经成为人类的宝贵财富。而信息系统作为信息采集、存储、加工、分析和传输的工具，已经成为社会发展的重要战略资源，信息系统的安全问题在信息化社会发展中越来越突出、越来越重要，已经成为社会发展中固有的重要问题，已关乎国家政治稳定、经济的发展、文化的繁荣和国防的建设。本章主要讲了信息的含义和特性，进而分析信息系统的概念、发展与功能，最后引出信息系统安全的概念及主要研究内容，这些基础理论为后面章节中提出的信息系统安全防护、避免安全威胁和不安全因素以及应用防范措施等起指导性作用。

1.5　习　　题

1. 简述信息、消息、信号的区别与联系。
2. 消息的含义是什么?
3. 信息的特性有哪些? 试举例说明。
4. 查找相关文献了解信息科学的 3 大基础理论。
5. 信息系统的主要类型有哪些? 各具有什么功能?
6. 信息系统安全的概念是什么?
7. 影响信息系统安全的主要因素有哪些?
8. 查阅相关资料了解信息系统安全领域的最新研究进展。
9. 简述信息安全、网络安全与信息系统安全的区别与联系。

第2章　信息系统安全工程ISSE及周期模型

20世纪90年代以来,伴随Internet在全球的普及,越来越多的组织将其业务过程转移或扩展到Internet环境下,与业务密切相关的信息系统安全的重要性受到广泛关注。面对各种网络攻击、病毒侵袭及内部人员误用等,已有的各种安全解决方案仍然不能保证系统的整体安全等级。信息系统安全工程的思想由此产生了。

2.1　ISSE概述

2.1.1　ISSE的基本概念

信息系统安全工程(Information System Security Engineering),简称ISSE,是侧重于信息安全的应用系统工程。ISSE是由NSA提出的为信息系统提供安全保障的系统工程技术,它用在设计和实现信息系统的过程中。ISSE是IATF中的重要组成部分。IATF是由美国政府和工业界联合提出的信息保障技术框架。此框架全面地概括了所有与信息系统安全问题相关的方面,包括系统工程、骨干网、本地计算环境、边界连接、支持系统等。ISSE为框架的其他部分提供了工程实现保障,是整个框架得以正确、完整实施的基础。

ISSE作为一种系统工程技术,不仅可以用来设计和实现独立的软硬件系统,还能为集成的计算机系统的设计和重构提供服务。ISSE与设计者和工程人员提供的设计要素,以及面向开发者、管理者、用户的接口相结合,在投资额度的限制下,使整体系统获得最大的安全性能。

ISSE是这样的过程:它解决用户的信息保障需求,是系统工程学、系统采购、风险管理、认证和认可以及生命周期安全的一部分。它是系统工程过程的自然扩展。这些过程都有公共要素:发现需求、定义系统功能、设计系统单元、开发和安装系统、评估系统有效性、系统采购、风险管理、认证和认可、生命期安全等。ISSE过程以使信息系统安全成为系统工程和系统获取过程整体的必要部分为目的,保证用户目标的实现,提供了有效的安全措施以满足用户需求,ISSE过程将信息系统安全的安全选项集成到系统工程中以获得最优的信息系统安全解决方案。

具体地说,信息系统安全工程是指将专门的安全技术(如通信安全、计算机安全和网络安全技术等)应用于信息系统生命周期的各个阶段,以保证组织对信息系统的需求按照可行的安全策略得到满足,并使信息系统能够抵御可感知的威胁。ISSE的工作范围包括:寻找与安全有关的设计要素,进行安全系统的预设计,设计安全系统规范,辅助详细设计,检查详细设计文档,评估方案与安全规范的一致性,推荐满足安全条件的部件,检查系统安装,设置性能测试等。ISSE将有助于开发可满足用户信息保护需求的系统产品和过程解决方案,同时,ISSE也非常注重标识、理解和控制信息保护风险并对其进行优化。

信息系统安全工程涉及一个综合的系统工程环境中与信息系统安全工程实践相关的各

个方面。为了使信息系统安全具有可实现性,必须把信息系统安全集成在系统生命周期的安全工程实施过程中,并与环境需求、业务需求、项目计划、成本效益、国家政策和标准等保持一致性。这种集成过程产生了一个信息系统安全工程过程,此过程可以确认、评估、控制和消除假定的或已知的安全威胁可能引起的安全风险,最终得到一个可接受的安全风险等级。

2.1.2　ISSE 的内涵

ISSE 是系统工程和方法论,是系统安全工程(System Security Engineering,SSE)、系统工程(System Engineering,SE)和系统获取(System Acquisition,SA)在信息系统安全方面的具体体现,是系统工程和系统建设的必不可少的组成部分,是对系统工程生命周期的安全风险控制。ISSE 并不是一个独立的过程,它依赖并支持系统工程,而且是后者不可分割的一部分。如图 2.1 所示。

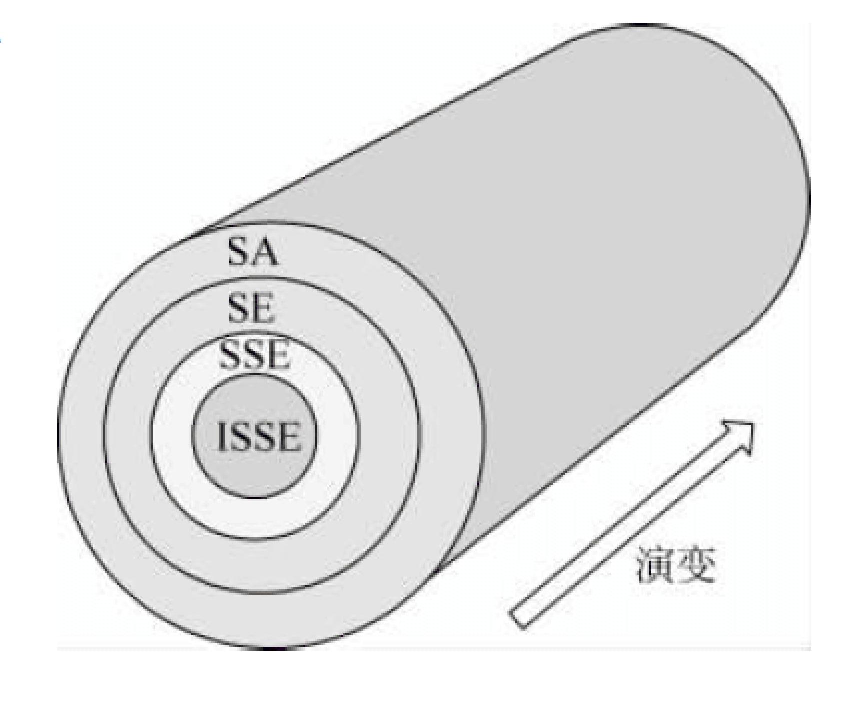


图 2.1　ISSE 与系统工程和系统获取的关系示意图

ISSE 是系统工程的子部分,它贯穿于系统工程的全过程,旨在对信息进行保护。ISSE 的主要工作最终体现如下:

(1) 描述并分析用户信息保障需求。

(2) 在系统工程过程早期,基于需求生成信息保障的要求。

(3) 确定信息保护的级别。

(4) 以一个可接受的信息保障的风险水准来满足要求。

(5) 建立一个基于要求的功能性的信息保障体系。

(6) 根据物理体系结构和逻辑体系结构分配信息保护的具体功能。

(7) 设计系统,实现功能构架。

(8) 部署信息保障体系。

(9) 根据系统的成本、进度和操作的适宜性及有效性等因素,平衡信息保障风险管理和其他 ISSE 事项。

(10) 研究与其他的信息保障和系统工程原则如何进行权衡。

(11) 将 ISSE 过程与系统工程和需求过程相结合。

(12) 测试系统,核实信息保障的设计,验证是否达到设计要求和信息保障要求。

(13) 在实施完成后进行用户支持,并根据其需求进行调整。

2.2　信息系统安全工程生命周期

在信息系统安全工程的每个主要阶段及其子阶段中,都要反复运用系统工程过程,包括需求分析、功能分析、综合分析、系统分析与控制。因此,在信息系统安全工程生命周期中完成过程实施需求(包括安全需求)时,就能有效地运用系统工程的基本原则。

在系统获取过程中，信息系统安全工程生命周期事件与系统获取的主要阶段之间的对应关系不一定是固定不变的。表2.1表示的是系统获取和信息系统安全工程各阶段的其中一种典型的对应关系。

表2.1 系统获取和信息系统安全工程各阶段的典型对应关系

系统获取各阶段	信息系统安全工程各阶段
先期概念阶段	先期概念阶段
概念研究和定义阶段	概念阶段
验证和证实阶段	需求阶段
	系统设计阶段
工程和制造阶段	初步设计阶段
	详细设计阶段
	实现和测试阶段
生产和部署阶段	配置审计阶段
运行和支持阶段	运行和支持阶段

信息系统安全工程生命周期主要包括9个阶段：先期概念阶段、概念阶段、需求阶段、系统设计阶段、初步设计阶段、详细设计阶段、实现和测试阶段、配置审计阶段、运行和支持阶段。下面将对信息系统安全工程的每一阶段做详细介绍。

1. 先期概念阶段

先期概念阶段的目的是确定用户的任务需求，指出开始构建一个信息系统应具备的安全能力，考察任务和分析任务。此阶段与系统获取中的先期概念阶段基本一致，都是确认任务要求。

在先期概念阶段结束时要提出一份有效的任务需求说明(Mission Needs Statement，MNS)。MNS通常由用户和ISSE人员起草。MNS作为系统获取过程生成的需求文档和规范的出发点，要能真正反映出需求的业务能力，因此需要仔细的考虑，但是也要避免过于详细地暗示某种方案。MNS中的内容不一定能完全实现，它只是一个目标。先期概念阶段涉及安全的活动如下：

(1) 根据如下活动，确定基于用户业务的、顶层的安全能力需求。

① 调查运行业务的问题。

② 对可能影响业务的威胁的一般性分类进行调查。

③ 找出由于国家和地方安全法律法规或政策造成的限制。通常只需指出政策标准，不必具体解释。

④ 确认业务环境安全目标的原始动力是业务需要还是政策需要。

(2) 在条件允许的情况下，初步识别责任认可者。

2. 概念阶段

概念阶段的目标是探索研究信息系统概念层面的安全方案，确定哪些方案可能满足任务需求，并从中选出需要进一步讨论的方案。

概念阶段进一步讨论一些能最好地满足要求，均衡调用资源，恰当地考虑限制的概念。概念阶段主要集中于评估系统概念，便于今后采取措施降低系统概念上的风险，同时使开发

者和用户都能理解系统的需求和问题。这点不同于系统需求阶段。信息系统安全建设的参与各方进行可选系统评审(ASR),对每个可能的代替方案进行审查,看其能否满足用户安全需求、是否符合有关的要求和规范,信息系统有关的所有问题都要调研,有冲突的地方都要解决。

在概念阶段结束时,得到信息系统工程建设和工程管理策略,以及初步的系统技术、成本、安全风险方面的情况。在下一阶段将进一步分析选出的系统概念,并正式确定系统需求。

在概念阶段,与 ISSE 有关的主要活动如下:

(1) 为系统威胁评估提供数据,预计系统不同阶段的安全威胁。

(2) 根据用户要求,提出与安全有关的用户运行需求描述。描述包括使信息系统安全运行的性能及其他功能要求,也包括由于国家、地方法规或政策造成的设计限制。

(3) 根据 MNS 评估技术、成本、进度、风险等内容,并为信息系统提供一份或多份安全备选方案。

(4) 提供生命周期安全计划、安全保障计划以及安全风险管理计划的数据。

(5) 确定是否需要新的信息系统安全方面的技术。

(6) 制定测评认证以及评估计划。

(7) 对安全风险进行初步评估,编写相关报告。

(8) 为认证与认可(Certification and Accreditation,C&A)提供相关的资料。

3. 需求阶段

需求阶段的主要目标是对概念阶段得出的信息系统安全需求和概念进一步发展,生成一份正式的信息系统安全需求报告,为信息系统的设计和测试做准备,使信息系统的使用者、获取办事机构及系统开发小组等对信息系统的需求有一致的理解。需求阶段通常出现在新开始的系统获取中,但在系统出现重大修改时也可能出现。

在需求阶段结束时,信息系统建设的各个参与者联合提出一份系统需求评审(System Requirements Review,SRR),SRR 是一份草案,内容包括系统所有的安全需求指标。

需求阶段比概念阶段需要更加严格的运行需求分析。一般都是由开发集成工程业务的合同承包商各负责一部分,并且更加面向工程人员。

在需求阶段结束时,要完成一份功能基线草案。正式的功能基线包括一份初步认可的文件,文件不仅描述了系统的功能、性能、互操作性、接口要求等,还给出了检验系统是否达到要求的手段。如果之前需求管理机制没有建立,此时需要建立。需求管理机制包括将来的需求,验证和证实(Verification and Validation,V&V)针对系统需求的设计和测试资料。

系统需求评审主要内容包括:充分考虑设计的限制,确认已经分析过的用户需求,并将用户需求进一步转化为有效的系统功能和性能需求以及安全方案;评估技术验证的方法和进程;识别和量化风险,对风险管理活动中的过程和方法进行评估;对系统的关键技术进行评估;评估并比较各种有效系统的需求;对系统说明草案以及相关的验证措施进行审查。

在需求阶段,ISSE 支持安全能力需求、安全目标、国家或地方的安全政策等安全需求必需的定义,是系统安全能力满足规定的要求。在需求阶段,ISSE 改进和完善了先前生成的安全需求、新的系统概念、安全风险评估等内容。

4. 系统设计阶段

系统设计阶段的目的是完成系统的顶层设计，并确定组成系统的配置项（Configuration Items，CI）和系统指标。它是正式工程活动和CI层面上管理的开始。

在系统设计阶段结束时，提出一份系统功能评审（System Functional Review，SFR）。SFR包含了正式开发开始前所必需的系统指标。系统设计阶段和以后的开发阶段都是由系统的开发小组来完成。

SFR的主要内容包括：确保系统功能需求和性能需求、约束条件、功能完备性及有关的限制，处理系统工程中的主要问题；评估新出现的物理体系和系统功能，使其满足系统功能和性能需求；更新和完善系统的功能和指标；确保提出的设计方案满足用户需求。

在系统设计阶段，与ISSE有关的主要活动如下：

(1) 分析系统的安全需求和配置项的安全需求，确保整个系统的安全需求都能得到满足。

(2) 继续进行安全设计，安全设计要支持系统层次体系、配置项定义、接口定义及其他产品采购方案。

(3) 完善系统的安全需求，检查是否有新的安全威胁并对威胁重新评估。

(4) 在SFR层次上，评审提出的系统设计安全方案的技术合理性。

(5) 详细地确定与信息系统安全验证和证实有关的需求和策略。

(6) 进一步考虑与安全运行和生命周期安全方面相关的问题。

(7) 审查系统特有的安全风险，必要的时候，进一步进行评估。

(8) 继续跟踪和完善与安全相关的工程管理计划和策略。

(9) 为认证和认可提供相关的材料。

5. 初步设计阶段

在初步设计阶段，当开发新系统或者对系统进行修改时，系统层面上的设计要求和指标被分配到配置项层面上。在这一阶段要提供初步设计评审（Preliminary Design Review，PDR）报告。PDR是基于配置项层面的评审，包括对每个系统配置项的硬件评审和软件评审。

PDR主要内容包括：找出在系统层面上未考虑的需求，以及未被配置项组件完全满足的需求；解决功能、配置项和子系统方面的问题；评审风险管理，确保风险在可接受的水平上；评估系统物理体系结构，确定内部和外部接口和互操作性方面的需求；识别集成后的系统设计，确保满足用户需求及功能基线需求。

在初步设计阶段，需要考虑系统各方面的问题，以及各问题间的相互关系。当成功地完成了PDR后，需要为绝大多数系统配置项建立分配基线。配置项的分配基线包括了一些初步认可的文件，文件描述了配置项的功能、性能、互操作性、同层间的接口要求、与上层的接口要求、设计限制、新的功能和性能要求，以及这些限制和要求被解决后的验证手段。此时初步设计阶段也就完成了。

在初步设计阶段中，与ISSE有关的活动如下：

(1) 评审配置项层面的参数和接口规范的定义及其他方面的问题，并进行改进。

(2) 对购买的CI或开发的CI进行验证，使其指标满足系统安全需求。

(3) 复查现有的安全方案，确保与 CI 需求一致。

(4) 为认证和认可过程继续提供资料。

(5) 检查系统各方面的问题。

6. 详细设计阶段

详细设计阶段的目标是完成那些没有现成品的配置项的系统设计。在详细设计阶段，首先要完成每个 CI 层面的关键设计评审(Critical Design Review，CDR)，然后根据每个 CI 层面的 CDR 得到整个系统的关键设计评审，即系统的 CDR。系统的 CDR 通常包括构成系统的各 CI 的具体设计，以及与软件和硬件相关的设计评审和文件。在开始实现最终系统以及测试之前，需要考虑到系统工程各方面的问题，以及各问题之间的关系。这点与上一阶段类似。

CDR 主要内容包括：找出配置项和关键设计都未解决的问题；考虑系统与其他系统的兼容性；确定 CI 设计和具体的系统是完整的；确定系统设计需求、接口需求和系统限制与可验证的结论保持一致，并进行证明；建立每个 CI 的分配基线。

在详细设计阶段，与 ISSE 有关的活动如下：

(1) 检查关键设计提出的安全方案的技术原理。

(2) 通过对关键设计安全方案、具体的软件和工程设计方案的评审，实现系统层面和 CI 层面的安全设计。

(3) 生成和验证信息系统安全的评估需求及测试，包括完整的系统、软件和硬件的测试策略。

(4) 确定每个 CI 的设计及 CI 间的接口设计能够满足系统的安全需求，并进行证明。

(5) 对与系统设计和开发有关的安全保障机构进行跟踪，并参与其中。

(6) 完成绝大部分生命周期安全保障方案的内容，包括新的培训资料和培训计划或应急培训计划的有关内容。

(7) 评审更新安全风险与威胁的预测，同时评审请求的任何修改动作。

(8) 提供认证和认可过程方面的资料。

在系统开发集成阶段，有足够的信息进行全面的安全评估。

7. 实现和测试阶段

在实现和测试阶段，开发一个新系统或者是对原系统进行修改，都需要准备好所有开发和非开发的 CI 产品，然后将所有 CI 产品集成为一个完整的系统，并检查确认集成的系统能够满足要求，另外也要检查系统进一步的生产和部署准备情况。在实现和测试阶段，同时也进行一些非常底层的设计活动。

在实现和测试阶段结束时，生成一份系统验证评审(System Verification Review，SVR)报告，在 SVR 中确认所建的系统与要求相一致，能满足任务的需求。在此阶段也要考虑系统工程各方面的问题，以及各问题之间的相互关系。

在实现和测试阶段，与 ISSE 有关的活动如下：

(1) 找出安全方案实现后系统和 CI 的安全需求与限制，以及相关的系统验证机制。

(2) 更新系统安全风险和威胁评估，并预测系统的使用寿命。

(3) 完善系统的运行程序和生命周期安全计划。

(4) 对与本阶段有关的安全保障机构进行跟踪和参与。

(5) 准备正式或非正式的 SVR 的安全风险评估。

(6) 为认证和认可过程提供资料。

(7) 最终检查系统的所有问题。

8. 配置审计阶段

配置审计阶段的任务是从系统层面进行评审,确保每个 CI 都进行了配置审计,比较建好的系统和前面各阶段的记录文件,文件记录了系统应达到的指标,并解决发现的大的问题或偏差。另外,配置审计阶段还要证实系统所有安全功能的实现都有文档记录。在本阶段结束时,生成一份物理配置审计(Physical Configuration Audit,PCA)报告。PCA 中包括所有配置审计的结果和解决系统出现问题或偏差的方法,并通过评审。

配置审计阶段结束时,为每个相关的 CI 建立产品基线,CI 可以是系统级 CI,也可以是作为组件配置的最低级别 CI。产品基线通常包括产品、过程和材料或资料的规范、工程图纸和其他相关数据。每个 CI 的产品基线包括一份初步认可的文件,也可能包括实际的设备和软件。初步认可的文件描述了 CI 的功能、性能、物理体系结构方面的要求;对 CI 作接收性测试时物理的和功能的需求;部署、支持、培训和拆除 CI 所需的测试。

在配置审计阶段,与 ISSE 有关的活动如下:

(1) 根据信息系统的安全需求,进一步评估相关的设计资料以及 CI 产品的指标。

(2) 最后确认系统的生产部署计划能满足信息系统安全需求。

(3) 最终确认系统运行安全规则和安全支持计划。

(4) 为认证和认可过程提供资料。

以上 ISSE 的活动的目的是支持系统层面的物理配置审计和功能配置审计(Functional Configuration Audit,FCA)。系统层面的 PCA 和 FCA 是为了评估系统层面上的需求,这些需求未被 CI 层面的 PCA 和 FCA 评估过。在配置审计完成,系统开始部署和运行时,一般要得到安全认可批准。

9. 运行和支持阶段

在运行和支持阶段,系统开始部署使用。运行和支持阶段要持续到系统拆除为止。从系统发挥作用到最终拆除,ISSE 确保系统安全得到维护,处理系统在现场运行时的安全问题,采取措施使系统的安全水平在系统运行期间不会下降。

在运行和支持阶段,与 ISSE 有关的活动如下:

(1) 监测系统物理配置和功能配置是否影响系统的安全风险。

(2) 对用户进行安全培训,并对安全培训进行评估。

(3) 监测安全部件的后勤支持,支持与安全有关的维护培训。

(4) 监测系统的安全性能,包括事件报告。

(5) 对与安全有关的部件的拆除处理进行监测。

(6) 监测与安全风险有关的因素,包括新发现的对系统安全的攻击、系统受到威胁的变化等。

(7) 评估各种系统改动对安全造成的影响。

(8) 为重新进行的认证和认可过程提供资料。

2.3　ISSE 过程

ISSE 是系统工程的子部分，它贯穿于系统工程的全过程，旨在对信息进行保护。ISSE 过程包括探索信息保障需求、确定信息保障系统、设计信息保障系统、实现信息保障系统和评估信息保障系统。

2.3.1　探索信息保障需求

“探索信息保障需求”是 ISSE 过程中的第一项活动。ISSE 首先要了解用户的工作需求、相关政策、法律法规、标准，以及使用环境中受到的威胁。然后 ISSE 确认信息系统及其用户、用户的行为特点、用户在信息系统生命周期各阶段的角色、责任和权力以及用户与信息系统交互作用的实质等。信息保障需求不能对系统的设计和实现造成过度的限制。

1. 所需完成任务的信息保障需求

ISSE 需要考虑系统信息可能从多方面受到的影响，包括人的因素和系统的因素，以及可能造成的各方面的损失。例如丧失机密性、完整性、可用性、不可否认性，或者它们的组合。

用户通常很清楚他们所需要的信息有什么用，但在发掘信息需要何种保障需求以及信息保障的优先级时遇到困难。为了探索出用户的信息保障需求，需要帮助用户弄清楚什么信息受到了何种破坏后会对总体任务系统造成危害。ISSE 需要做的是：

(1) 帮助用户对信息处理过程建模。

(2) 帮助用户定义对信息的各种威胁。

(3) 帮助用户确定信息保障需求的保护级别。

(4) 设计信息保障策略。

(5) 与用户达成一致，获取用户许可。

确定用户需求是 ISSE 实施的与用户交互的活动，确保任务需求中包含信息保障需求。ISSE 在设计信息保障系统时需要评估信息对任务的重要性，并遵循用户的意见。这一阶段要达到的目标是：一份满足用户在成本、性能、时间等各方面要求的信息系统保障框架。其中至少包括以下方面：

(1) 被处理的信息的类型是什么？

(2) 谁有权力处理信息？

(3) 授权用户如何处理以及使用何种工具处理？

(4) 用户行为是否需要监督？

(5) 系统中是否有不可否认性需求？

在这个阶段，ISSE 的工作需要用户的参与，否则很难做出令用户满意的决定。

2. 对信息系统的威胁

ISSE 将信息威胁作为设置保护级的出发点，然后定义安全服务的类型。对信息系统的

威胁是指在某些实体进行了某些活动后,引发了对系统造成危害结果的潜在性。ISSE 需要在用户的帮助下,准确、详尽地定义出在系统的设计、生产、使用、维护以及废弃的过程中可能受到的威胁。

3. 考虑信息保障策略

对信息系统而言,在制定信息保障策略时,除了了解需求和威胁,还要考虑现有的信息保障政策、法律法规和标准。信息保障策略主要需要定义出信息保障的内容和目标、信息保障的职责落实、信息保障的方法。为达成上述目标,策略制定小组不仅需要系统工程师、ISSE 工程师、用户代表,还需要信用机构、认证机构、设计专家,甚至是政府机构的参与。

信息保障策略必须由高层管理机构批准并颁布,它是分层的。一旦制定后,高层的策略一般是不会改变的,而下层的局部策略是可以根据具体情况而定的。在策略的执行过程中,应使每个参与者都能够理解策略。如果策略在某些地方不能得到执行,则需要让其他参与者知道。还需要有一个能够确保实施策略的流程,并让参与者认识到违反该策略将会出现的后果。

2.3.2 确定信息保障需求

在确定信息保障系统的过程中,用户对信息保障的需求和信息系统环境将被细化为对象、需求和功能。这一过程将确定信息系统将要做什么、如何去执行其功能以及信息保障系统的内部和外部接口。

1. 信息保障对象

信息保障的对象与通常的系统对象具有相同的特性,例如对于信息保障需求的确定性、可度量性、可验证性、可追踪性等。每个对象的基本原理都要说明下列性质:

(1) 支持信息系统中的任务对象。

(2) 驱动与任务相关的威胁。

(3) 存在的意义。

(4) 支持对象的信息保障策略。

2. 系统内部关联和环境

系统内部关联和环境是指系统与外界交互的功能和接口,包括物理上的和逻辑上的。任务对象、信息的特性、信息处理、威胁、信息保障策略等因素都极大地影响着系统环境。系统内部关联和环境对于确定系统边界并实施保护是很重要的。

3. 信息保障的需求

ISSE 需求分析的任务是评审和更新此前工程过程中的分析,包括任务、威胁、对象、系统内部关联和环境。系统需求中应规定出系统必须完成的事情,而不是去设计和实现系统。系统需求的分析中必须定义系统的功能要求和设计约束。ISSE 和其他信息保障系统的所有者主要检查正确性、完整性、一致性、依赖性、冲突和可测试性。

2.3.3 设计信息保障系统

目标系统已经明确后,就可以进入信息系统的设计阶段,ISSE 将构造系统的体系结构。

ISSE 工程师将继续进行下述工作：

(1) 对安全需求和威胁评估进行细化和检查。

(2) 确认底层的需求能够满足系统级的需求。

(3) 支持系统级架构配置项和接口定义。

(4) 继续跟踪、细化信息保障需求。

(5) 确定信息保护完整性的验证策略和步骤。

(6) 考虑信息保护操作。

(7) 继续进行信息保障系统风险检查与评估。

1. 功能分析

功能分析要将此前的要求分析阶段所确定的高层功能分解至低层功能，与高层功能相关的性能要求也要分解至低层。功能分析的结果是描述每个产品或项目的逻辑功能或性能。当某种系统功能被定位到某个系统部件或人身上后，信息保障功能也就附上了系统元素。此描述通常称为信息保障系统构架。

2. 信息保障预设计

在需求和构架已经确定后，ISSE 进入了信息保障的预设计阶段。实施信息保障预设计的最小条件是具有在配置管理下的稳定的信息保障体系结构。ISSE 工程师将制定出系统建造的规范，ISSE 在这一阶段的行为至少包括：

(1) 检查、细化需求和预期成果，尤其是系统配置项和接口规范的定义。

(2) 调查已有解决方案，使之与配置项要求相匹配。

(3) 验证配置项层的方案与上层方案相一致。

3. 信息保障详细设计

详细设计将进一步完善配置项层方案，细化底层产品规范，检查每个细节规范的完整性、兼容性、可验证性、安全风险、可追踪性等。要做出合理的设计决策，需要 ISSE 不断地实施评估，以比较系统安全需求中的预期风险。信息保障详细设计包括以下内容：

(1) 检查、细化配置项层方案。

(2) 提供具体的设计资料以支持配置项层和系统级的设计。

(3) 检查关键设计的合理性。

(4) 设计信息保障测试和评估程序。

(5) 实施信息保护保障机制。

(6) 验证配置项层的方案与上层方案相一致。

(7) 提供各种测试数据。

(8) 检查、更新信息保障的风险和威胁。

2.3.4　实现信息保障系统

这一阶段的目标是通过采购、配置、测试、记录和培训，使系统从设计转为运行。除此以外，在这一阶段，ISSE 所执行的其他用于实现和测试信息保障系统的功能还包括：

(1) 验证系统能够防御威胁评估中确定的威胁。

(2) 验证信息保障方案，实施系统验证，确定是否与需求和环境相符。

(3) 跟踪信息保护保障机制在系统实现和测试活动中的运用情况。

(4) 审查系统的生命周期计划、运行流程以及培训材料,并向这些文档提供数据。

(5) 实施正式的信息保障评估,为最终的系统有效性评估做准备。

上述这些信息将为后来的安全验证提供帮助,安全验证之后一般还会有安全信任审核。

1. 采购部件

通常,决定组件是自行生产还是采取购买的方式,可根据偏好进行选择。影响决定的因素包括可操作性、性能、成本、时间进度、风险等。其他因素包括系统组件的依赖性效果、组件的最低性能对系统性能的影响以及组件在将来的可用性。ISSE 判断已有的产品是否能满足系统部件的需求,最好能有多种产品可供选择。另外,为确保系统实现之后仍具有较强的生命力,ISSE 还应考虑将新技术运用到系统之中。

2. 建造系统

信息保障系统同许多系统一样,必要的保护机制是否在系统中实现,会直接影响系统的最终效果。作为信息保护系统,还需要格外注意:

1) 物理完整性

对设备、组件是否有物理安全保护措施。

2) 人员完整性

组装、建造系统的人员对工作流程是否具有足够的知识和适当的涉密许可级别,以保证系统的正确性和可信性。

这些是容易被忽略而又非常重要的并且会影响系统安全性的因素。在构建系统时应当给予足够的重视。

3. 测试

ISSE 要给出与信息保障相关的测试计划和工作流程,还要给出测试实例、工具、软硬件等。测试将验证子系统或系统的性能。测试计划应考虑单个组件和整个系统测试所需的人员、工具、设施、成本及进度等问题。此阶段的工作包括:

(1) 检查信息保障系统的设计结果并改进。

(2) 验证系统层和配置项层的信息保障需求和环境限制,以及实施方案和相关的系统验证和确认机制和决策。

(3) 在系统实现和测试过程中跟踪并应用系统保护保障机制。

(4) 审查系统生命周期安全计划,包括后勤、维护和培训计划。

(5) 持续实施风险管理工作。

2.3.5 评估信息保障系统

ISSE 也强调信息保障系统的有效性。有效性评估着重针对系统在机密性、完整性、可用性和不可否认性等安全特性方面。如果系统在这些方面达不到设计要求,就很难满足用户的需求。其中的重点包括:互操作性、可用性、培训、人机接口和成本。

互操作性是指系统是否通过外界接口正确地对信息进行了保护;可用性是指系统是否能给用户提供信息和信息保护;培训是指用户需要何种程度的培训才能正确地操作和维护

信息保障系统；人机接口是指用户错误操作或削弱保护机制；成本是指构造和维护系统的资金是否可承受。

2.4　ISSE 的基本功能

本节主要介绍与 ISSE 工作相关的各种典型活动以及 ISSE 的基本功能。ISSE 活动一般是系统工程中的子过程。ISSE 的每项基本功能都包含了许多高技术的特殊活动。ISSE 小组参与的主要活动包括：系统总体控制、分析和规划，需求分析，系统设计，系统开发集成，验证，运行，为有安全需求的系统提供生命周期安全计划。这些活动必须由拥有足够经验和专门技能的系统工程师和安全专业人员来进行指导和完成。

在整个系统生命周期的每个阶段，信息系统安全工程小组参与的活动并行地、反复地执行。各活动之间是相互协调的。在每一阶段，每项活动需要的技术项目等级也不同。当活动涉及到证明活动成果的概念和信息时，除了生命周期运行和支持活动外，在这个阶段的开始，多数活动就要求付出极大的努力，同时也需要巨大的资源开销。在过程中期阶段，提炼和更新信息，并把信息变换为可实现的系统方案；在过程中期阶段前期，实现概念或信息并进行验证，证实有效后即可投入到长久的运行使用中；在过程中期阶段后期，使用和支持概念或信息，并在必要时对它们进行修改，最后进行部署。在过程早期和中期阶段的预期过程和获取程序本身安全需求的过程中，安全运行分析和生命周期活动就已经开始了，但是关于运行和生命周期安全功能的大量工作主要在后期阶段完成。该阶段需要进行部署、使用、监控、支持，并根据系统的安全特性而进行有效修改。ISSE 基本功能、生命周期各阶段和系统事件如图 2.2 所示。

ISSE 过程包括一系列安全工程功能，这些功能与系统工程各阶段或事件相对应。通过反复运用图 2.2 的基本过程，实现了各工程间的相互协调。在图 2.2 中，每一横格代表了一个基本的 ISSE 功能，每一纵格代表系统生命周期的一个阶段。在每一阶段结束后，生成相关的系统事件，如 MNS、ASR 等。图 2.2 中横格和纵格的交叉说明了在系统的任一阶段，ISSE 的每一基本功能都要考虑到。

在系统开发的不同阶段涉及 ISSE 各功能的程度也不一样。每个 ISSE 功能至少有 3 种模式：为实现功能作准备；实现功能；当系统发生变动或有新情况出现时要做出相应改变。

项目不同，对应的每一阶段所花费的时间和精力也不同。但在一般统计情况下，在系统开发的前 5%的时间内，系统生命周期中 85%的时间和精力开销就已经确定，这就说明了大量的时间和精力消耗在生命周期开发之后，消耗在系统运行和支持阶段和对系统的修改中。因此，系统的所有相关人员应尽早讨论和分析贯穿系统生命周期的有关问题。ISSE 过程的目的是找到解决问题的工程方法。

从图 2.2 中可以看出，ISSE 的基本功能包括安全规划、控制和 ISSE 小组形成，安全需求，安全设计，安全运行，生命周期安全和安全风险管理。

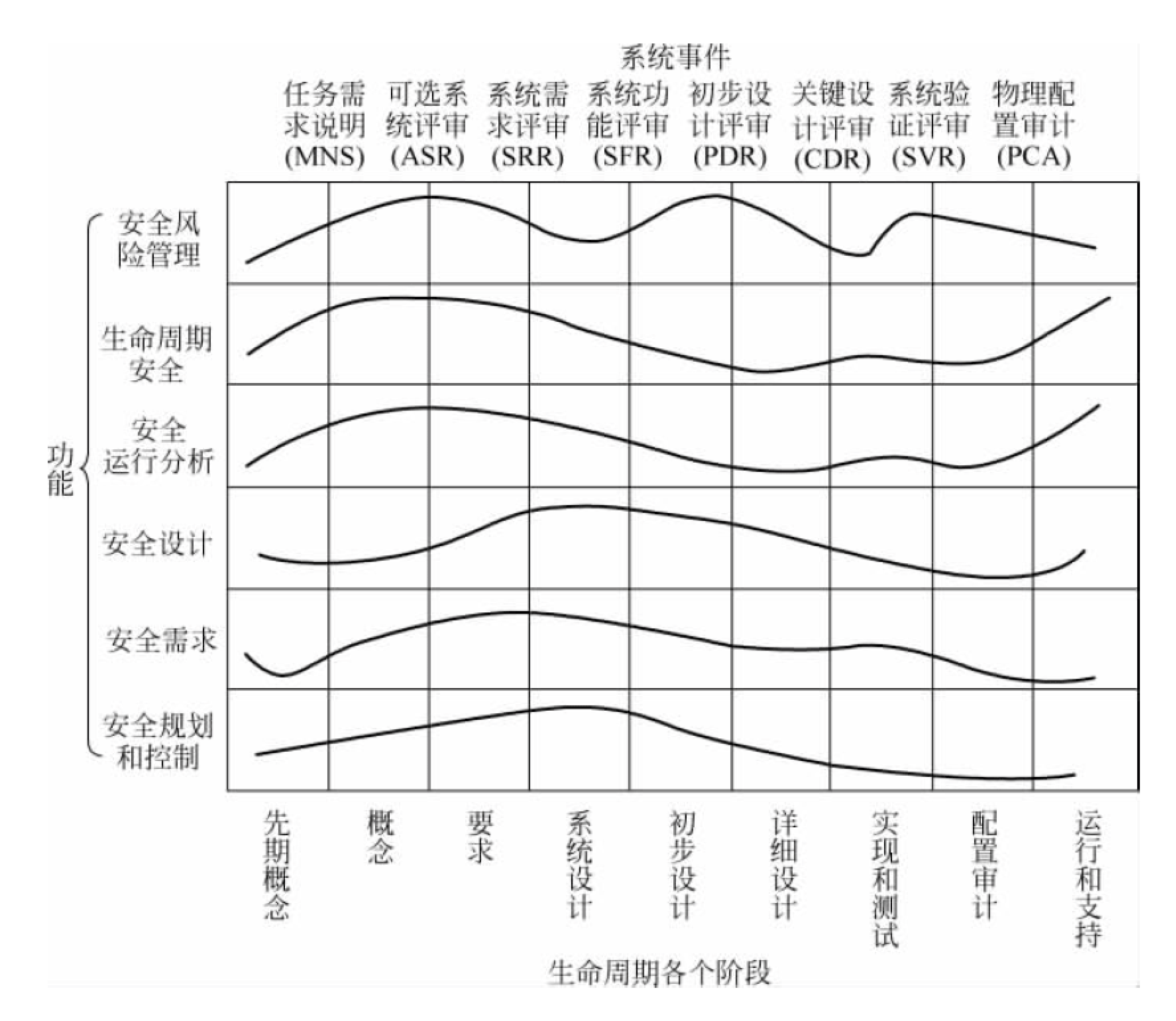


图 2.2 ISSE 基本功能、生命周期各阶段及系统事件

2.4.1 安全规划、控制和 ISSE 小组形成

系统和安全工程管理以及规划活动应该在工程开始时就启动了。它们是 ISSE 功能的基本部分。为了系统地把安全需求嵌入到有效的设计中，应尽早开始规划活动并很好地提供强有力的资金支持。

一项重要的活动就是要成立由系统安全工程师领导的小组，以便综合和协调安全规划。在系统工程小组内确定 ISSE 的需求，针对这些需求成立 ISSE 小组，并提供必要的工具和资料。相关的安全规划活动还包括组合参与协作工程过程的客户和 ISSE 执行人员，达到系统的安全目标及成本、进度和操作运行的目标。有效准备和规划能保证恰当的信息系统安全工程输入会在系统工程过程的最佳点被接收，并且提供给适合的小组成员。ISSE 小组在未来需要提供适当的计划来适应扩展的或新的用户业务需求、系统发展需要和技术。

成立 ISSE 小组的目的是协调信息系统安全工程，使其满足可操作性、低成本和符合进度安排目标。在制定总体系统工程管理计划(System Engineering Management Plan，SEMP)时，ISSE 小组同系统项目办事机构(SPO)一起工作。SEMP 是一份综合性文件，文件描述如何管理和实施全面的综合性工程工作。与 ISSE 小组相关的主要功能角色及其关系如图 2.3 所示。

在图 2.3 中，关键管理专家包括 INFOSEC 技术工程师，INFOSEC 威胁分析员，INFOSEC 客户服务代表，理论、政策和发布专家，系统安全剖析工程师及安全评估员。其中安全评估员可以包括系统分析员、软件分析员、技术安全分析员、密码分析员、信号分析员、安全故障

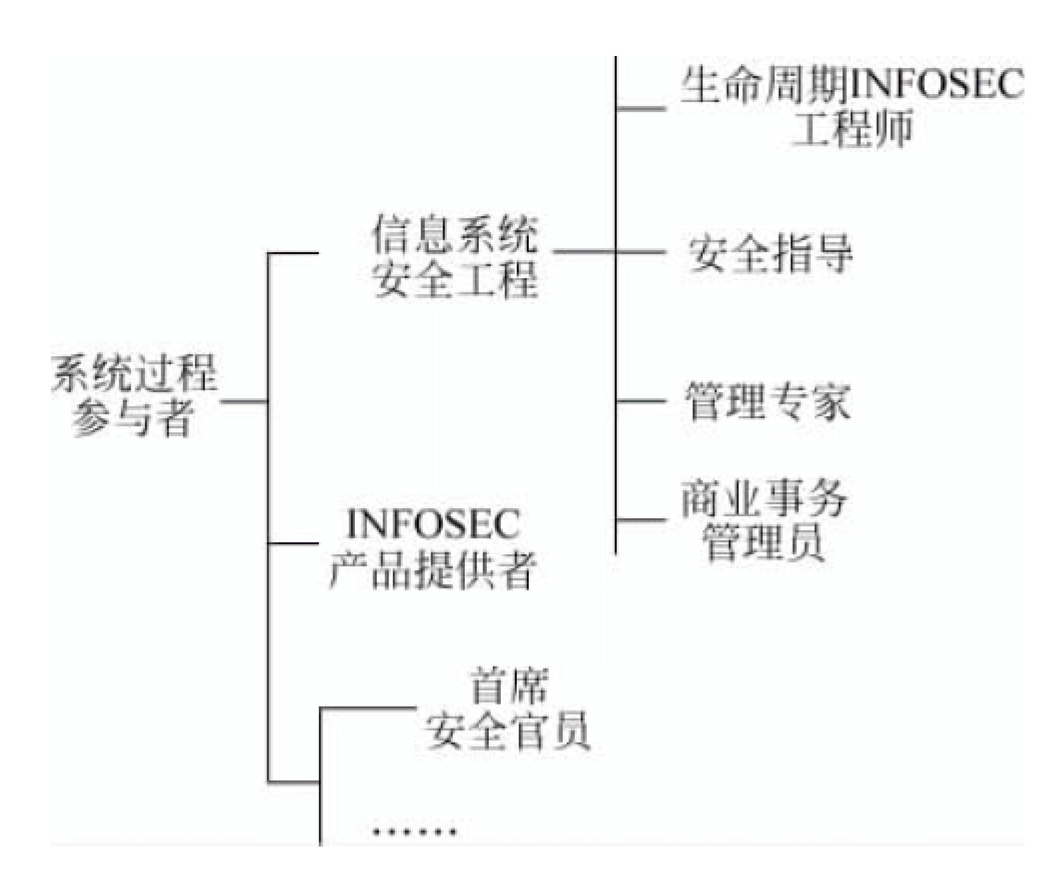


图 2.3 信息系统安全工程小组的功能角色及其关系

分析员及密码验证分析员等。

ISSE 小组首先要与客户建立良好的关系和沟通手段，目的是理解工程的目标、成本和进度、项目的过程方法以及系统工程结构。当不能实现使用物理方法进行沟通的时候，可以通过自动化和电信业务的虚拟方法进行联络，也可以通过站点访问。对于 ISSE 小组在系统工程的作用以及如何与系统用户、系统开发小组和 C&A 小组进行协作，ISSE 小组要和客户达成共识。当客户尚未配备安全专员与 ISSE 小组进行相同级别问题的讨论时，双方应共同商定以何种方式克服沟通障碍。选择方案如下：

(1) 使用批准的联络站作为中介。

(2) 提升客户的许可级别。

(3) 使用在技术层面上的方式向客户提供信息，但是不包括尚未得到授权的信息。

ISSE 小组也要与物理的、管理的、人事的、运行安全的负责人和组织建立良好的工作关系。

从完成开发直到系统具备完备的运行能力为止，信息系统安全工程小组都要参与。在初始开发周期即将结束时，需要指定生命周期信息系统安全工程师(Life-Cycle INFOSEC Engineer，LCIE)。LCIE 可以是来自信息系统安全工程小组派出机构的人员，可以是其他安全人员，也可以是来自客户或最终用户机构的人员。当系统进入运行和支持阶段时，LCIE 接管信息系统安全工程小组的领导权。在需要时，LCIE 可以得到其他技术专家的协助。从系统投入现场运行到系统废弃阶段，LCIE 都可以向用户提供支持。当系统被报废后，支持就结束了。

下面介绍本阶段的主要工作。

1. 商业决策和工程规划

商业决策的一个结果是指定信息系统安全工程小组成员和首席信息系统安全工程师。在做出正式的商业决策之前，可由信息系统安全客户代表履行信息系统安全工程师的职责。

首席信息系统安全工程师在商业规划过程中，阅读已有的文件，并与客户就小组安排和支持需求进行讨论，然后准备一份小组成员配备预案。商业决策应作出与支持 ISSE 相关的支出的预算。支出可能包括以下几项：设备支出、差旅支出、工程工具支出和相关支持服务支出。

其他工程策略活动还包括确定进度、合同文件和工程文档策略的规划以及相关的安全验证和确认活动。若某些因素发生重大变化，则ISSE小组需要报告给决策者，以便确定对工程协议进行修订。

ISSE小组还应考虑与安全C&A小组的关系。

对于急需的或非常大的项目，可能需要多人来充当ISSE小组成员的角色。如果项目较小，可能要求首席信息系统安全工程师充当ISSE小组的多个甚至是全部的功能角色。ISSE小组成员的实际数量，基本的信息系统安全人员，以及他们各自的工作水平根据工程的规模、敏感性和可用资源的相对优先级的不同而不同。

2. 规划ISSE对认证和认可的支持内容

ISSE小组同客户一起工作，以便尽早确认系统的指定批准机构(Designated Approving Authority，DAA)和其他安全C&A小组参与者，然后再与管理机构、测评认证机构沟通，规划ISSE对C&A的支持内容。

认证和认可是针对信息系统和其他保护措施的技术性或非技术性安全特征而进行的一种综合评估，目的是确定某一特定设计和实施能够满足已指定的安全需求的程度，并由DAA正式声明某信息系统被批准可在某一可接受的风险水平上运行。

理想情况下，安全认证活动应在系统生命周期各阶段完成。测评认证要与风险评估相关联，在系统生命周期内由C&A测评人员不断地评审和修正，并确定剩余风险。安全认可(Security Accreditation)的规划应在系统生命周期开始阶段完成。如果C&A小组无特别要求，ISSE小组应为C&A提供必需的全部信息系统安全信息和产品，以完成安全认证工作，并取得安全认可决策。ISSE小组应同C&A小组一起工作，以最大限度地减少在认证分析和相关证据搜集方面的重复工作。

初始的认证任务包括系统构架分析、软件设计分析、网络连接是否符合规划分析、集成产品的完整性分析、生命周期管理分析和漏洞评估。

进行认证和认可的系统要有支持每个任务的正式文档、安全规范、测试和评估综合计划(Test and Evaluation Master Plan，TEMP)以及确保所有网络与其他互连要求均被实现的书面说明。可以定制针对系统的认证任务，以适合系统的项目战略和生命周期管理过程。

最终的认证任务包括安全测试和评估，渗透测试，TEMPEST和RED-BLACK核实，确定是否符合通信安全标准，系统管理分析，站点认可调查，意外事件应急计划评估和基于风险的管理评估。

ISSE小组为C&A提供的内容包括：

(1) 安全目标和安全需求的描述。

(2) 安全保障计划。

(3) 与安全相关的信息，包括接口规范。

(4) 与外部系统接口作用的信息。

(5) 安全威胁分析报告。

(6) 安全需求验证的可跟踪矩阵(Requirement Verification Traceability Matrix，RVTM)或相关决策数据库信息。

(7) 系统安全运行计划、方案和其他分析。

(8) 生命周期安全计划。

(9) 安全测试或其他验证计划和数据。

(10) 安全风险评估或风险评审报告。

(11) 实用产品安全特性文件和产品安全评价报告。

(12) 测评认证机构人员的介入。

(13) 系统安全评估和特征数据。

信息系统安全工程也应了解其他形式的系统验收决策，并提供数据资料。例如，如果用户拥有系统过渡或验收计划，而计划中的过渡时期的决策者不是 C&A 安全测评机构的人员，系统总体验收机构会充当安全认可者的角色，安全认证活动由 ISSE 小组来完成。

3. ISSE 报告

1) 用户或同级小组报告

ISSE 小组应随时向客户通报所承担的工作和进展情况，并传达需要提醒客户注意或进行讨论的问题。在有可能的情况下为客户进行适当的演示，作为定期现场访问或是工程技术评审。这将有助于修正在项目实施中发现的问题。

2) 机构的管理报告

在每一个重要项目里程碑评审之前，ISSE 小组为机构管理人员提供简报，给出有关技术和状态的信息，保证管理部门拥有管理和支持 ISSE 过程必需的信息。工程初期简报讨论如何裁剪 ISSE 过程来适应客户的需要和安全能力需求，以及小组完成了什么活动。

在没有异常安全风险或实施小工程项目时，ISSE 小组在重要项目技术评审之前非正式地发出近期管理简报，或者使用电子邮件每周或每两周发送简明的书面报告，也或者每周或每两周同监督人员一起讨论进展情况。然而在实施具有较高风险的项目时，ISSE 会比较深入、频繁地向上级管理部门汇报情况，但每季度或每半年才提交正式的小组报告。

简报大致包括的内容有：

(1) 证明 ISSE 小组遵循了原定的 ISSE 过程，向管理部门提供工作质量和成果方面的建议。

(2) 评审用户的运行以及安全能力需求等方面的工作。

(3) 确定 ISSE 小组已经完成了的活动，并与先前简报中的工作计划比较。

(4) 有关信息系统安全支持和成果的反馈。

(5) 系统描述。

(6) 建议的安全方案。

(7) 安全风险评估结果。

(8) 进度情况。

(9) ISSE 人员配置和其他资源问题。

(10) 技术策略变化或早期简报得出的风险数据。

根据简报，管理部门能够判断经过裁剪的过程是否适用，用户是否满意 ISSE 小组的工作。

4. 技术数据库和工具

1) 决策数据库

系统工程确定一种使用和维护技术数据库的方法，可以是一种记录或是在线工程数

据库。决策数据库是系统工程数据的集合。决策数据库在系统需求和方案改进时维持它们当前状态的快速记录和历史记录。ISSE小组按要求向系统决策数据库提供信息并从系统决策数据库获取信息，包括直接访问系统数据库或采用硬拷贝或电子方式交换信息。

一般情况下，决策数据库包括以下内容：

(1) 综合的系统需求和对配置项的下行配置。

(2) 接口限制和要求。

(3) 系统概念、初步设计和详细设计选择方案。

(4) 选定设计的全部文档。

(5) 验证。

(6) 决策准则。

(7) 商业研究评估。

(8) 原理图集。

(9) 模型和仿真。

(10) 设计图和详图。

(11) 配置文档和变化控制手段。

(12) 可跟踪性审计追踪。

2) 知识库的开发和重用

ISSE小组利用和充实信息系统安全知识库，使ISSE过程更有效、更正规。ISSE专业人员可通过以下渠道对知识库进行开发和重用：

(1) 与同级工作人员、高级技术领导和管理人员非正式地分享ISSE思想、经验和输出。

(2) 传播经过质量检查的运用示例。

(3) 为在线或联机资料库进行数据库输入。

(4) 经验报告。

(5) 张贴在电子公告牌上的非正式评注。

(6) 列出参考资源的工作帮助信息。

(7) 丰富ISSE培训课程的信息。

(8) 专业技术和工具。

(9) 正式发行指南和技术论文。

通过上述渠道可以达到知识共享。

3) 工具的选择和使用

自动化工程工具的选择和使用非常重要，可能影响到ISSE功能的技术规划。很多的工具可以用于需求定义、设计、软件和硬件实现、测试和分析、运行方案建模、技术文档发布和工程管理等。ISSE小组可以使用与系统开发小组直接兼容的技术工具实现信息共享。

5. 与采购和签约有关的规则

1) 采购策略

采购策略是指选择最适合该工程和工程环境的系统的获取策略。采购策略规划了ISSE小组同系统项目办公室(SPO)的关系，以及需要承包商支持的程度。采购策略需要考虑的问题包括：

(1) 最适合的承包合同。

(2) ISSE 小组参与承包合同的监控的时间。

(3) ISSE 为支持承包合同所需要的费用。

(4) 把信息系统安全有关材料精练为系统技术标准或工作说明(Statement of Work, SOW)所包含的参考资料,如指南、标准、准则、保证等。

(5) 每个相关合同或任务订单的合同数据要求的原始材料。

(6) 合同修改和工程变动对 ISSE 的影响。

(7) 为技术性能提供的信息系统安全的素材。

(8) 将信息系统安全需求输入到技术性能的度量集合中。

(9) 合同的安全技术规格要求——承包商使用的安全登记指南;承包商个人许可证等。

2) 预先规划的产品改进策略

预先规划的产品改进策略(Pre-planned Product Improvement Strategy, P^3I)是对已获取系统所做的计划的未来改进。该策略把重大风险推迟以便在以后的工作中开发,其原因可能是无法负担的费用或者技术原因。

3) 工程文档编制规划

编制的文档涉及几乎所有的安全问题,如系统级和产品级技术规范、系统测试计划、获取和后勤支持计划。

6. 信息系统安全保证计划

信息系统安全保证计划是用与信息系统安全相关的保证技术把安全功能需求同相关的可测度的强度级别或依赖级别结合到一起。实现安全保证的技术包括测试、分析、过程控制、评审和其他开发。安全保证计划是一种方法,它用来确定用户保护什么,如何将它划分等级,然后如何保证给予它同等级的安全保护。ISSE 小组协助制定信息系统安全保证计划。安全保证计划包含一张在系统生命周期应用的安全保证技术清单里,每项安全保证技术的时间和范围都包含在这个计划内。安全保证计划信息应包含在系统文档中。

由于并非构成系统的所有功能都要求相同的强度和可信度,因此安全保证计划应当确定安全保证等级的级别,如“低”、“中”、“高”,并描述每个级别的相关技术和标准,还要描述集中应用该技术的特定环境。为了确定安全保证等级,ISSE 小组和客户共同确定一个负面的安全结果清单,即违背安全需求的事件,并对清单进行排列和分类,每个类别都要有清晰的安全可信级别,在此级别上负面的结果将不会出现。确定的安全保证等级与抵御潜在敌方攻击等级及其技术能力、投入资源的能力和动机相关联。

在这方面国家应当制定一些适用于 ISSE 的安全保证需求的公用标准(如橘皮书)。

2.4.2　安全需求

安全需求定义是指采用某种方法描述用户对信息系统安全的要求。定义方法有两种:形式化定义和非形式化定义。传统的做法把安全作为非功能需求之一,附加在系统需求分析之后进行,且大多采用非形式化定义方法。形式化定义则是借助数学工具来精确描述安全需求,建立适当的安全策略模型,便于安全设计、实现和验证。对信息系统安全的可用性、可审计性、身份认证和防否认性尚无较好的形式化定义和策略模型。John McDermott 和

Chris Fox 提出一种采用妄用例模型(Abuse case model)捕获和分析安全需求的模型。妄用例(Abuse case)被定义为系统与一个或多个操作者之间的一类交互,交互的结果对系统或操作者或系统的所有者是有害的。Mariana Gerber 等则提出一种采用二维矩阵的安全需求定义方法,其中第一维定义信息系统安全问题的百分比分布,第二维描述安全事件的后果对服务、产品和业务过程的影响,也是通过提问的方式得到百分比。将上述二维结合起来,形成矩阵,最后确定组织对安全问题的需求,并分为低、中、高 3 个档次。关于安全需求的内容将在第 4 章详细展开。

2.4.3 安全设计

安全设计是信息系统安全的重要内容,它是根据系统的安全需求,设计系统的整体安全框架,提出系统在总体方面的策略要求、各个子系统应该实现的安全技术措施、安全管理措施等,形成用于指导信息系统具体安全建设的安全方案。安全设计包括物理实体安全设计、硬件系统和通信网络安全设计、软件系统和数据的安全设计等内容。从 ISSE 的角度来看,安全周期的各个阶段包含安全设计。关于安全设计内容将在第 5 章详细展开。

2.4.4 安全运行

安全运行分析是确保信息系统正常运行的必要环节,它影响产品、过程和系统安全需求的解决方案。安全运行概念分析和定义是系统工程和 ISSE 过程的综合,为认证和认可提供关键数据。

在系统生命周期内,安全运行分析要有以下形式的文档:

(1) 设计评审说明。

(2) 培训材料和文件。

(3) 人的接口要求。

(4) 系统环境假设规范。

(5) 程序和政策文档。

以上文档需要进行提交评审。

安全运行概念、理论和过程解决方案的开发,从概念阶段开始,并持续到配置审计阶段,在系统进入运行期后,这一开发将继续并进一步演变,理论分析最终变成了实际的运行模式。

反复应用于系统生命周期内的安全运行分析集中在以下几个方面:

(1) 确定与其他系统进行交互的环境要素。

(2) 确定扮演的角色,如系统用户、系统维护人员、系统管理员、假定的威胁代理。

(3) 确定自动化角色,如数据源点、数据发散点、远程应用操作员、网络服务命令发起者。

(4) 确定在其任务环境中与操作系统交互的方法和方式。

通常,安全运行分析不包括与系统结构和行为有关的内容,也不包括可见的外部自动化接口。计算机存储器的精确配置通常与安全运行分析无关。

需要考虑的典型运行情况有:

(1) 在正常和不正常条件下启动和关机。

(2) 系统和人对错误条件或安全事件的环境反应。

(3) 系统或组件失灵时,要在预先计划好的退化方式下维持运行。

(4) 可在不同模式下运行。

(5) 对安全事件或自然灾害的响应、恢复模式。

(6) 系统对关键性和常见的内部和外部事件的反应。

安全运行涉及的分析角色包括:

(1) 用户。

(2) 安装者、维护者。

(3) 管理者。

(4) 威胁代理。

2.4.5　生命周期安全

虽然安全计划可以在系统生命周期的任何时刻制定,但是建议在系统生命周期的开始阶段制定,包括理解安全需求、参与安全产品评估并最终实现系统的工程化设计及实施。安全与信息系统的其他方面一样,对整个信息系统生命周期各阶段都进行计划是最好的管理方式。信息界长期以来认同的原则是,系统设计完成后在其中增加安全特性比在系统初始的设计阶段包含该特性要多花费十倍的时间。在系统开发之后再改进安全解决方案将更困难,通常成本也更高,而且还很可能打断系统的持续运行。安全也需要融入到信息系统生命周期的后期,以协助确保安全能够跟得上系统环境、技术、规程和人员的变化。它还确保在系统升级时考虑到安全问题,包括采购新的部件或设计新的模块时。在安全入侵、灾难或审计后对系统增加新的安全控制会造成无计划的安全实施,这种实施比一开始就将安全集成到系统中要更昂贵和缺乏效率,而且还会严重地降低系统的性能。当然,事先考虑到系统生命周期中所有的问题实际上也是不可能的。所以,通常至少应该在生命周期每个阶段结束时,或每次重新审批后更新系统安全计划。对于许多系统,可能需要更频繁地更新,产生一个反复式的系统开发生命周期。

信息系统生命周期模型有很多,但是大多包含 5 个基本阶段。

(1) 起始阶段。

在起始阶段,表述系统的需要并记录系统的目的。

(2) 开发或采购阶段。

在这个阶段对系统进行设计、购买、编程、开发或其他形式的构建。这个阶段经常包含所定义的其他周期,如系统开发周期或采购周期。

(3) 实施阶段。

在初期的系统测试后,系统被安装到位。

(4) 运行和维护阶段。

在这个阶段系统执行其工作。几乎总是要对系统进行修改,增加硬件、软件或发生其他大量的事情。

(5) 废弃阶段。

当完成向新系统转移的工作后,旧系统被废弃。

系统项目办公室与用户一起开发一些机制以提供维护系统安全状态的长期能力,也就

是监督在系统整个生命周期各阶段的计划，包括开发、生产、现场工作、维护、培训和拆除。

本节主要介绍信息系统生命周期的安全活动。

1. 起始阶段

确定系统概念和早期设计过程通常涉及新系统需求的发现；系统特征的初期建议和所推荐的功能；关于系统体系结构、功能和性能方面的讨论；以及环境、财政、政治或其他方面的约束。同时，系统安全方面的主要问题应该在系统设计早期考虑，可以通过敏感性评估来进行。

敏感性评估既考察所处理信息的敏感性，也考察系统本身的敏感性。评估应考虑法规要求、机构政策以及系统的功能需要。敏感性通常以机密性、可用性和完整性表示。在评估敏感性时需要考察系统对机构使命的重要性，系统或数据的非授权泄露、更改或无法使用的影响这类因素。为了处理这些问题，系统的拥有者、使用者和安全评估的评估者应该参与评估。

敏感性评估应该考虑以下问题：

(1) 系统处理的信息。

(2) 数据或系统的错误、非授权泄露、更改或无法使用造成的潜在损害。

(3) 影响安全的法律或法规。

(4) 系统或信息对于威胁的脆弱性。

(5) 特别考虑的环境因素，如系统处于危险的位置。

(6) 用户拥有的安全知识，如技术掌握和培训水平或安全许可证。

(7) 适用于系统的安全标准、法规或指导方针。

2. 开发或采购阶段

1) 确定安全需求

在开发或采购阶段的初期，系统计划者定义系统的需求，安全需求与此同时制定。系统安全需求与其他系统需求一样，是从法律、政策、适用的标准和指导方针、系统的功能需要，以及成本效益的平衡取舍等方面导出的。确定安全特性、保证和运行措施可以获得大量的安全信息。对这些信息进行确认、更新并将其整理为系统设计者或购买者使用的、详细的安全保护需求和规格说明。

2) 生命周期安全的开发方法

ISSE 小组、LCIE 和客户一起，为系统整个生命周期定义一个可理解的安全方案。由于某些系统的安全需求可采用非技术的过程而不是技术产品解决方案，在开发阶段以及运行阶段要与负责系统安全的各种机构建立密切关系。这些机构可能有助于场地勘测、物理和管理安全分析及对策分析。

ISSE 小组、LCIE 和客户、C&A 小组要一起制定系统生命周期的安全计划。对 ISSE 小组来讲，要考虑的问题如下：

(1) 在开发、测试和使用期间对系统进行监控，以确保与安全需求持续一致，不能在可接受范围之外增加额外的风险。

(2) 系统培训一定要涉及安全特性和限制，这样才能保证在日益增多的安全风险中操作和维护产生错误的可能性受到控制并且可以接受。

(3) 追踪与安全有关的组成单元的处理指令，使其遵守相应的法规和规则，不能增加安全风险。

(4) 保证配置管理过程是适当的，以避免在无适当批准的情况下使安全风险上升。

(5) 确定与系统偶然性运行计划相匹配的系统安全偶然性计划，以便使系统可以承受更大的风险。

(6) 为系统提供安全评价，专门发现系统的安全漏洞和薄弱环节，弥补这些安全漏洞和薄弱环节，提高系统安全防护能力。

(7) 保证后勤和维护能够支持系统中与安全有关的组件的需求，使其不能引起安全风险的增加。

生命周期对安全的主要目的是确保系统的保护手段在运行和支持阶段依然满足其安全目标。要明确提出引起不可接受安全风险的已知缺陷，并采取修改措施进行弥补。对于安全违规，安全检查或安全审计中发现的安全缺陷，或授权期满，都要进行修改。

直接或更宽范围内环境的改变影响系统安全形势和解决方案的变化有：

(1) 任务和被保护的信息重要性或敏感性改变，可能导致安全需求和要求的对抗措施的改变。

(2) 威胁的改变使系统的安全风险增加或减少。

(3) 应用的改变要求不同的安全操作模式。

(4) 发现新的安全攻击手段。

(5) 破坏安全、破坏系统完整性或通过揭示安全缺陷使授权无效的异常事件或小事件。

(6) 新的安全审计、检查和外部评价结果。

(7) 系统、子系统或组成单元配置的改变或修改。

(8) 排除或降低配置项。

(9) 排除或降低系统过程的对抗性措施。

(10) 与新的外部接口相连。

(11) 运行环境的改变。

(12) 新对抗技术的应用。

(13) 系统安全授权期满。

3) 系统安全监控的部署

系统安全功能在系统运行期间应能被连续监控，并通过生命周期安全把问题提前设计到系统中。ISSE 小组进行折中研究以确定什么样的监控手段可以提供最好的成本—效益比并在可接受的风险范围内。

3. 实施阶段

在一些生命周期计划中可能没有特定的实施阶段。它通常被纳入开发和采购的后期或运行和维护的前期。

1) 配置管理

配置管理是对系统变化进行控制的过程，系统包括硬件、软件、文档、测试设备等。建立一个配置控制委员会(Configuration Control Board，CCB)，用于审查和批准系统的修改。CCB 成员包括 ISSE 小组、LCIE、C&A 或其他相关的信息系统安全代表。

在系统整个生命周期内，实行配置管理的原因包括：

(1) 系统在不断变化和演变。

(2) 在生命周期内的某一给定点上维持一个基线。

(3) 偶然事件造成的毁坏。

(4) 对 C&A 证据的追踪。

(5) 系统资源的有限集合在使用期内将增长。

(6) 配置项的身份证明。

(7) 配置控制。

(8) 配置会计学。

(9) 配置审计。

ISSE 小组保证系统配置的过程在系统生命周期内都保持工作状态,并以信息系统安全为关键目的。CCB 成员参与配置过程,并发现和评估对安全有影响的改变。

2) 安全测试

系统安全测试包括对所开发或采购的系统特定部分的测试和整个系统的测试。物理设施、人事、规程、安全管理、商业或内部服务(如网络服务)的使用以及应急计划是对整体系统安全产生影响的例子,但它们可能处于开发或采购周期之外的领域。因为只有在开发或采购周期之内的部分才会在系统接收测试中得到测试,所以可能需要对这些额外的安全组件进行独立的测试或审查。

3) 审批

系统安全审批是审批人员对系统运行的正式授权和对风险的明确接受。它通常由对系统管理、运行和技术控制等的检查支持。检查可以包括详细的技术测评、安全测评、风险评估、审计或其他此类检查。如果生命周期过程被用于管理一个项目,如系统升级,认识到审批是针对整个系统而不仅是新增部分是很重要的。

审批过程迫使管理者做出提供充分安全防范措施的关键决定。基于技术和非技术防范措施的有效性以及残留风险的可靠信息所做出的的决定更可能是个好决定。在决定安全防范措施和残留风险的可接受性后,审批人员发表正式的审批意见。在某些情况下,可能会临时执行审批,允许系统运行并在过渡期结束时接受检查,这时就完成了安全升级。

4) 安全培训

信息系统复杂性、统一性、开放性、互联性在给人们的工作和生活带来方便的同时,对信息的安全也构成了严重的威胁。因此加强用户信息系统各类人员安全意识和安全技术的培训是当前确保信息系统安全运行急需采取的一项重要措施,也是信息系统安全工程的重要内容。

建立一套完整的培训体系,能够为员工提供满足组织需求并适用于系统工程活动的、及时有效的知识与技能培训。以项目的要求、组织的战略计划和现有的员工技能情况为指导,确定组织在技能与知识方面所需的改进。

培训是整个系统生命周期内所必需的。培训就是要培养具有安全资质的信息系统安全保障人员,以满足信息保障不断变化的需求。ISSE 小组鼓励用户参与对系统正确配置、维护和安全特性使用的有关培训活动。这种培训可以针对系统管理员、系统开发者、系统维护人员、机构执行官、安全官员、安全认证者或评估者等。培训人员要具备执行赋予他们的角色的技能与知识,并要根据培训计划和编制的材料进行人员培训。培训课程需要进行审核,

以便确定其中是否包含与安全相关的培训材料。培训完成后要评估培训的有效性以满足所确定的培训要求。评估有效性的方法应与培训计划编制和培训材料的拟定同时列出并及时获取有效性评估的结果，以便对培训做出相应调整。要对培训记录进行维护以追踪每个人员接受培训的情况，以及受训后的技能和能力。通过培训，使其具备专业技能、相关知识、所需管理能力，使其在信息系统以及信息基础设施受到威胁时进行有效的预防、阻止和响应。

培训内容包括：系统的操作流程和方法；安全意识、基本安全技术知识和安全管理知识；系统维护和安全功能的使用；安全管理制度和管理流程；系统安全事件的应急处理流程和恢复流程。

4. 运行和维护阶段

1）后勤和维护

ISSE 小组应保证后勤支持需求是在考虑系统的安全需求后开发的，并保证这些安全需求在系统的后勤计划中被提出来。需要给出所要求的任务、设备、技能、人员、材料、服务、供应品和程序的定义，保证系统最终项目的提供、存放和维修。如果没有良好定义的过程，并持续使用不合适的工程和系统分析技术，系统的质量和可靠性在运行和维护过程中可能恶化，导致维护和运行费用的增加。

后勤支持是管理和技术活动经过训练的、统一和反复应用的方案，管理和技术活动是下列活动所必需的：

（1）集成后勤支持到系统和装备的设计中。

（2）开发与备用项目、设计有关的支持需求。

（3）获取必要的支持。

（4）以最小的代价在运行期间提供必要的支持。

2）系统更改

系统及其运行的环境会发生持续的更改。为了响应诸如用户的抱怨、出现新的特性和服务或发现新的威胁和缺陷，系统管理者和用户需要修改系统并增加新的特性、新的规程和对软件进行升级。

系统运行的环境也会更改。网络和网络互连有增加的趋势。可能会增加新的用户组，这可能是外部用户组或匿名用户组。新的威胁可能会出现，如网络入侵的增加或个人计算机病毒的扩散。如果系统有配置控制委员会或其他管理系统技术更改的机构，可以安排安全专家在委员会中工作以便就更改是否影响安全做出判断。

当发生或计划更改时，要决定更改是较小的还是重大的。重大的更改，如重新设计系统的结构，会极大地影响到系统。重大更改经常涉及购买新的硬件、软件、服务或对新的软件模块进行开发。

（1）较小更改。

对系统的更改无须进行深入分析，但还是需要一些分析。每一个更改都可以进行有限的分析来衡量优点（收益）和缺点（成本），这甚至可以在会议中当场进行。即使进行非正式的分析，决定还是应该被适当地记录在文档中。在这个过程中，即使是“很小”的决定也最好是基于风险做出的。

ISSE 小组在计划和开发较小更改时，必须和客户紧密合作。较小更改往往是系统运行和维护基金内可以处理的或者得到机构运行资金支持的更改，较小更改的开发活动远比系

统开发规模小。ISSE 小组应参与到这些更改中，以保证可接受安全风险等级的系统安全状况不能因更改而降低。对于提议的系统更改，ISSE 小组应基于需求的更改特性做出判断。

(2) 重大更改。

有时可能需要对系统进行一处或多处更改，甚至完全替代系统。当需要大量新的资源、特殊或大规模采购或大规模工程人力资源时，需要改变系统的大部分或特别关键部分时，就认为是重大更改。

重大更改需要进行分析以确定安全需求，分析可能仅仅集中在发生或将要发生更改的领域。如果在整个生命周期中原来的分析和系统的更改都被记录在文档中，分析工作一般会很容易进行。因为这种更改源自重要系统的获得、开发工作，或政策的更改，所以应该重新审批系统以确保残留风险仍然是可接受的。

5. 废弃阶段

废弃阶段涉及信息、硬件和软件的处置。信息可以转移到其他系统、存档、丢弃或销毁。当存档信息时应该考虑未来取回信息的方法。用于创建记录的技术在未来可能无法随时获得。硬件和软件可以被出售、赠送或丢弃。除了一些包含保密信息的存储介质只有用销毁的方式清除以外，很少有硬件需要被销毁。如果有必要，软件的处置应遵循许可证和其他与开发商的协议。一些许可证是针对站点的或包含防止软件被转移的其他协议，也可能要采取措施对数据进行加密以便将来使用，如采取适当的步骤确保对密钥的长期和安全存储。

系统的废弃处置，还应考虑到短期和长期可能破坏环境和伤及人与动物健康的影响。系统工程处置功能还包括再生、材料恢复、废物利用，以及对开发和生产过程中副产品的处置。ISSE 小组应保证为系统所制定的处置计划要充分考虑到该系统生命周期的有关安全方面的问题。

2.4.6 安全风险管理

1. 安全风险管理概述

信息系统存在安全隐患，需要有安全意识和行为来防范。安全风险管理(Security Risk Management，SRM)，是一个条理化的分析过程，目的是确定在什么情况下可能产生错误，评估安全风险以及实现处理安全风险的手段。安全风险管理确定可接受的风险、评估风险的当前程度、采取措施将风险降低到可接受水平。

安全风险是对达到技术性能、成本和进度方面的目的和目标的不确定性的一种度量。安全风险等级是用安全事件和安全事件出现的概率来分类。风险源包括以下几个方面：

(1) 技术方面。

可行性、可操作性、可生产性、可测试性、可维修性、技术和材料的可获取性和系统的有效性。

(2) 进度方面。

技术材料的可用性、技术成果和里程碑。

(3) 资源方面。

资源的利用率和资源的保护程度。

(4) 合同方面。

进度和成本。

传统的安全风险管理的方法有两种：反应性方法和前瞻性方法，它们各有优缺点。

(1) 反应性方法。

当一个安全事件发生时，很多 IT 专业人员感到唯一可行的就是进行遏制，指出发生了什么事情，并尽可能快地修复受影响的系统。有些会试图确定根本原因，但是对于那些在极端资源限制条件下的人而言，似乎是不可能的。反应性方法是一种对已经被利用并转换为安全事件的安全风险的有效技术响应，使反应性方法具有一定程度的严密性，可帮助所有类型的组织更好地利用他们的资源。

最近的安全事件可帮助组织预测将来的问题并做好准备工作。这意味着如果组织以一种平静且理性的方式来响应安全事件，并且确定允许事件发生的根本原因，则能够更好地保护组织在将来不受类似问题的伤害，并且能更快地响应可能出现的其他问题。

(2) 前瞻性方法。

与反应性方法相比，前瞻性安全风险管理有很多优点。与等待坏事情发生然后再做出响应不同，前瞻性方法首先最大程度地降低坏事情发生的可能性。通过制定计划、实施控制来保护组织的重要资产，这些控制减少被恶意软件、攻击者或偶然误用等利用漏洞的风险。组织不应完全放弃事件响应。有效的前瞻性方法可帮助组织显著减少将来发生安全事件的数量，但是似乎此类问题并不会完全消失。因此，组织应继续改善他们的事件响应流程，同时制定长期的前瞻性方法。

风险管理是包括以下 4 个阶段的循环。

第一阶段：风险的识别与评价。

第二阶段：风险的分类。

第三阶段：制定对应的风险控制方案。

第四阶段：执行方案。

(1) 风险的识别与评价。

风险识别是风险管理的基础，也是风险管理的第一步。只有正确识别出自身所面临的风险，才能主动选择有效的方法进行处理。风险可以是多种多样的，风险识别的任务就是从错综复杂的环境中找出系统所面临的主要风险。风险识别可以通过感性认识和历史经验来判断，也可以通过对各种客观资料和风险事故记录来分析、归纳和整理，以及进行必要的专家访问，从而找出各种明显和潜在的风险及其损失规律。因为风险具有可变性，所以风险识别是一项持续性和系统性的工作，要求风险管理者密切注意原有风险的变化，并随时发现新的风险。

风险评价是对系统发生事故的危险性进行定性或定量分析，评价系统发生危险的可能性及其严重程度，以确保最低的事故率、最少的损失和最优的安全投资效益。

(2) 风险的分类。

风险分析之后，对风险进行分类、整理，然后考虑控制对策。可以把风险分为 3 大类。

第一类：发生频率低且每次发生损失额小，此类风险可无视它，不需特别的对策和控制。

第二类：经常发生的风险，如系统不能正常运行。对此类风险，要分析选取可行的控制

方案。

第三类：指火灾、地震等不常发生的灾难，发生的概率很低，一旦发生损失相当大。对此类风险，要正确估计发生的概率是相当困难的，但要充分重视，万一发生，损失极大。

(3) 执行风险控制方案。

在完成了风险分析之后，ISSE 需要比较所有备选的行动方案，深入分析各类相应的安全对策是如何改善和减缓当前风险状态以及系统的任务功能的。基于风险分析，决策者决定风险控制方案。决策的基础是威胁和脆弱性风险、风险对策成本和任务的功能性，以及风险对策减缓整个风险的有效性。ISSE 将记录参与风险的情况。

(4) 执行方案。

信息系统只有在该系统是运行在本地的 DAA 可接受的风险级别时才算完成。它通过验证和确认来实现。

验证是确保系统能够满足已经声明并文档化的需求的过程。确认是指再次检验系统是否达到规定的目标，系统能否全面实施。

2. 安全风险管理计划

安全风险管理是 ISSE 过程中的一个子过程，并贯穿于系统的生命周期内，它是集成在 ISSE 过程中的重要组成部分。在系统开发早期，ISSE 小组就要制定系统生命周期内的安全风险管理计划。只要 ISSE 小组认为适当，安全风险管理计划就应集成到现有的与安全有关的项目计划中去。

在安全风险管理计划中，安全风险要考虑的主要因素包括：

(1) 覆盖给定系统生命周期过程的安全风险管理策略。策略可由正式的安全风险评估委员会的活动构成，也可由简化的安全风险评审构成，或者两者兼有。

(2) 安全风险文档，即综合安全风险评估报告。

(3) 收集传播安全风险信息计划，即安全风险管理期间的密级分类规则。

(4) 建立项目每个阶段的授权的风险验收机构以验收剩余风险，审查 SRM 发布的文档。

(5) 确认 SRM 活动要求的人员及其扮演的角色。

(6) 估计 SRM 活动要求的总体工作量。

安全风险评价委员会的活动包括：

(1) 客户请求。客户可以请求风险评估来帮助做出安全判决。

(2) 新项目安全风险基线的确定，包括安全策略、运行安全需求和任务环境设计的基本安全要求。

(3) 在系统生命周期的关键点上，为做出合理决策，可能启动风险评估。

(4) 增加新的客户需求替代方案。

安全风险信息和文档内容包括如下：

(1) 所有可能的案例、事件、攻击的信息以及不能使系统保持与期望的安全需求相一致的脆弱性。

(2) 特定系统出现的风险和可能性的评估。

(3) 使项目计划缓解和运行环境得到改善的手段。

(4) 活动进程的建议。

安全风险计划的任务目标可以归纳为以下 5 点：

(1) 理解信息保障需求。

(2) 体现风险状态。

(3) 体现什么可以做。

(4) 决定将要做什么。

(5) 执行决定。

3. 安全风险分析

安全风险分析方法如图 2.4 所示，图中列出了一个安全风险分析模型，该模型包括在 C&A 材料中，可供安全认证参与者参考。

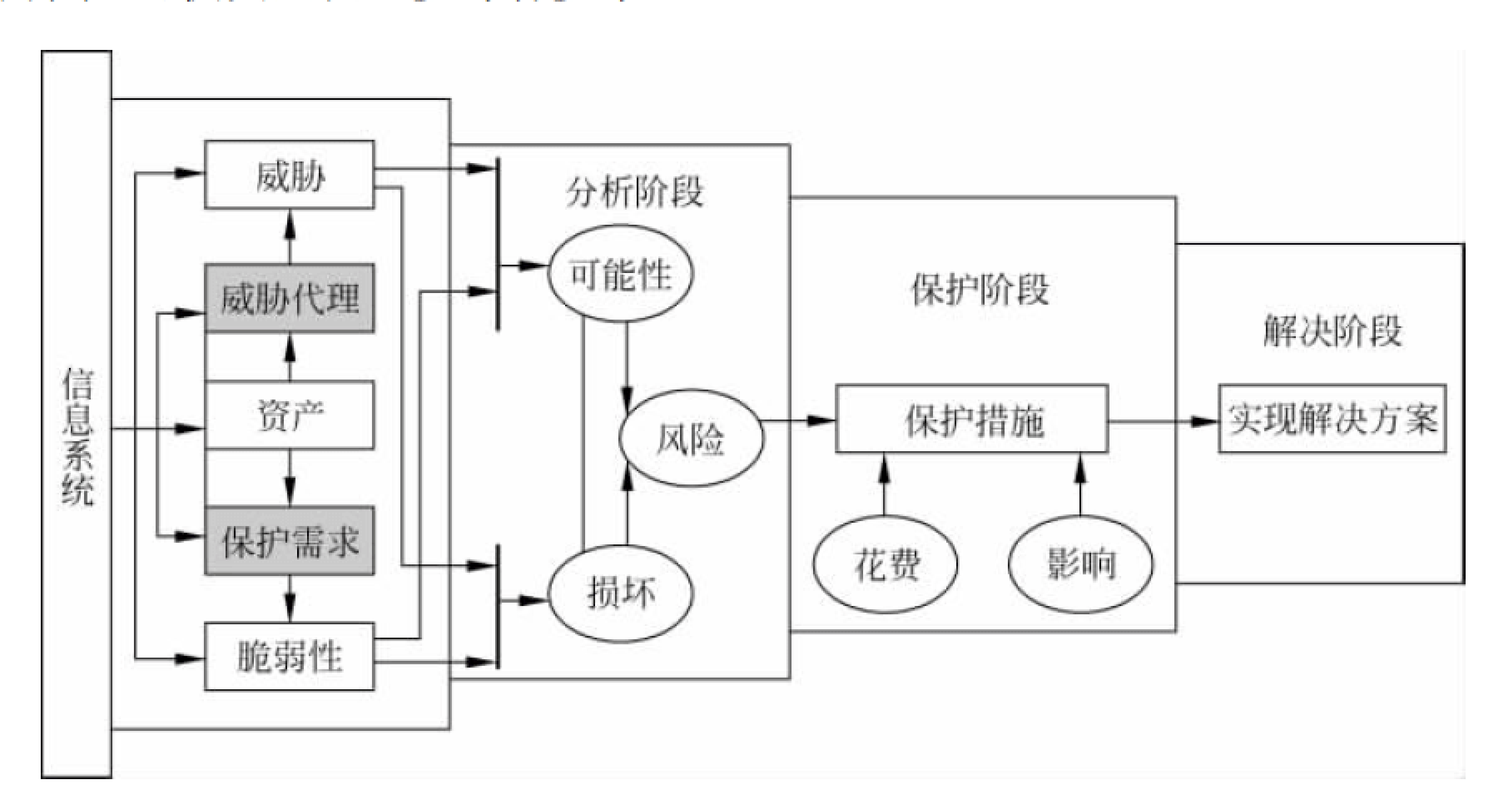


图 2.4　安全风险分析方法

由图 2.4 可以看出，安全风险分析步骤如下：

(1) 分析信息系统。

(2) 确定资产并识别。

(3) 识别保护需求和威胁代理。

(4) 识别威胁和脆弱性。

(5) 确定威胁和脆弱性的可能性和潜在的破坏。

(6) 计算风险。

(7) 确定保护措施。

(8) 实现解决方案。

2.5　本章小结

本章首先简要介绍了与信息系统安全工程相关的概念，然后详细介绍了信息系统安全工程的生命周期各阶段及各种典型活动。所有这些活动必须在 ISSE 小组的指导下完成。接着介绍了信息系统安全工程的过程。概括描述了安全规划、控制和 ISSE 小组形成、安全需求、安全设计、安全运行、生命周期安全、安全风险管理等信息系统安全工程的基本功能。

2.6 习　　题

1. ISSE 的基本概念是什么?
2. 简述 ISSE 的生命周期。
3. 简述 ISSE 的过程。
4. ISSE 的基本功能是什么?
5. 简述安全规划、控制和 ISSE 小组形成的内容。
6. 简述决策数据库的内容。
7. 简述信息系统安全工程中培训应注意的问题。
8. 简述安全风险分析过程。

第 3 章　信息系统安全规划

3.1　信息系统安全规划概述

随着社会信息化程度的不断深入与提高，我国各地区、各行业使用信息系统开展工作的比例越来越大，信息系统安全问题也日趋严重，安全问题逐渐成为影响业务运行、制约生产力发展的重要因素之一。信息化的发展将面临着信息安全方面的严峻考验，对信息系统安全进行全面的规划以适应形势发展的要求已经是一个不能回避的问题，也将成为人们共同关注的保证信息安全的重要环节。

信息系统安全规划是信息系统在未来几年内如何达到系统安全需求指导下的安全建设目标的一个过程。信息系统安全规划应该是一个依托信息化战略规划，涉及物理安全、网络安全、系统安全、运营安全以及人员安全的信息系统安全的总体规划。

3.1.1　信息系统安全规划的概念

信息系统安全规划是信息化规划的重要组成部分之一，它所要完成的主要任务是围绕信息系统的发展规划，从网络安全、应用安全和管理安全 3 个层面，根据调研结果提出信息系统的信息安全需求，参照国内外相关标准，制定信息系统的信息安全规范，建立信息安全体系结构(包括信息系统安全体系结构和信息安全管理体系)，并提出一套有效的信息安全保障措施和测评技术。

信息系统安全规划是一个涉及管理、法规和技术等多方面的综合工程。信息系统安全的总体目标是物理安全、网络安全、数据安全、信息内容安全、信息基础设备安全与公共信息安全的总和。信息系统安全的最终目的是确保信息的机密性、完整性和可用性，以及实现信息系统主体对信息资源的控制。

信息系统安全规划是以信息化战略规划为指导，以信息资源规划为基础，全面完整地规划信息系统应用和相关信息架构，确定信息系统的安全框架、管理模式与建设步骤。只有在信息系统安全规划的指导下建设的网络与信息环境，才可以在安全机制的控制与制约下，让各种业务解决方案、应用系统和数据都不受负面因素带来的威胁并在其上实现有效配合。信息系统安全规划不应该只是规划未来几个月，而应该规划未来几年内如何达到信息化远景规划指导下的安全建设目标。信息系统安全规划比单独购买信息安全产品更重要，只有通过有计划、有方向、有目的、有配合地进行信息系统安全的整体布置，才能构成真正意义上的信息安全。

信息系统安全规划主要是根据风险评估的结果和提取的安全需求描述实施相应的安全保障的目标、措施和步骤。按照“全网安全”的思想，信息系统安全规划需要从管理、组织和技术等多方面进行综合考虑，涉及的是综合管理、技术规范和运行维护等多个层面的控制

措施。

信息系统安全规划的范围应该是多方面的，涉及技术安全、规范管理和组织结构。技术安全是人们谈论比较多的话题，也是在安全规划中描述较多的地方，用得最多的一些安全产品，如防火墙、入侵检测、漏洞扫描、防病毒、VPN、访问控制和备份恢复等。但是信息系统安全是一个动态发展的过程，过去依靠技术就可以解决大部分安全问题，现在仅仅依赖安全产品的堆积来应对迅速发展变化的各种攻击手段是不能持续有效的。信息系统安全建设是一项复杂的系统工程，要从观念上进行转变，要在安全产品的支持下建设全方位的安全策略，使之成为一个可持续的、动态发展的、有安全保障的渐进过程。因此，在目前安全设备达到一定规模的情况下，规范管理就成为信息系统安全规划需要关注的核心内容，在信息系统安全规划中一定要将规范管理放在首位。规范管理包括风险管理、安全策略、规章制度和安全教育，这几个组件是信息系统安全规划的重要内容。信息系统安全规划需要有规划的依据，这个依据就是信息化战略规划，同时更需要组织与人员结构的合理布局来保证。没有合适的人员配合工作，任何事情都是不可能完成的，因此，在安全规划中不可以忽视组织结构建立和人员合理调配这个关键环节。

通常情况下安全规划设计包括安全需求分析、安全总体设计、安全建设规划 3 个主要环节。

(1) 安全需求分析。

首先根据系统的安全级别选择和确定系统基本安全要求指标，然后根据安全要求指标评估系统安全现状，找出系统安全现状与安全指标之间的差距，并进行额外的风险评估，找出系统的一些特定需求，两者结合后形成系统需求分析报告，建立系统安全需求。

(2) 安全总体设计。

首先根据系统风险评估结果和系统安全需求制定系统总体的安全策略，然后根据总体安全策略和等级保护的相关要求，设计系统的安全技术框架和安全管理框架，形成既符合系统安全等级保护要求，又满足系统特定安全保护需求的安全总体设计方案。

(3) 安全建设规划。

首先根据系统的总体设计方案选择安全建设的策略，然后根据安全建设策略，规划中长期的安全建设内容，制定安全建设的实施计划，形成指导今后一段时间安全建设工作的安全建设规划方案。

3.1.2 信息系统安全规划的目标

信息系统的安全规划应该以国家和地方政府的法律法规为前提，遵循国内外的相关标准和规范，围绕信息系统的发展规划来制定信息系统安全规划，使得信息系统建设和运营满足国家安全体系的要求。

信息系统安全规划的目标与信息系统的安全目标是一致的，集中体现为信息保护和系统保护两大目标。信息保护目标主要保护所属组织的敏感信息和系统运行中有关信息的机密性、完整性、可用性和可控性。系统保护的目标主要是保护所属组织的运行和实现职能的技术系统的可靠性、完整性和可用性。无论是信息保护还是系统保护，信息系统安全规划的目标集中起来其实就是 CIA(Confidentiality，Integrity，Availability)。对于致力于信息安全研究的人来说，CIA 代表了信息系统要达到的目标，是信息系统安全规划的统一

目标。

C 代表保密性(Confidentiality),目的是阻止敏感信息的泄露和未授权用户的非法访问。I 代表完整性(Integrity),防止未授权用户对系统信息进行的有意或无意的修改。A 代表可用性(Availability),保证授权用户在需要时可以成功访问系统及其数据信息。

3.1.3　信息系统安全规划的原则

信息系统所面临的威胁大体可分为两类：一是对系统中信息的威胁；二是对系统中设备(包括软件和硬件)的威胁。影响信息系统安全的因素很多,有些因素可能是有意的,也可能是无意的；可能是人为的(如黑客),也可能是非人为的(如设备、线路故障)。但是从安全防范角度来分析,信息系统安全规划所涉及的对象可以分为两种类型：重要应用系统和公共支持系统。在实践中根据这两种类型的特点来分别制定信息系统安全规划是一种行之有效的办法。在一个大的信息系统内部通常包含多个应用和多种计算机与网络设备,如果属于重要应用系统或公共支持系统的应用或设备,那么就必须对其制定专门的安全规划。对于已经运行的系统,则应根据已制定的安全规划定期进行安全评估。对于其他应用无须制定专门的安全规划,这些应用的安全问题可由其运行环境中的公共支持系统的安全控制来保证。一般而言,标准的商用软件,如字处理软件、浏览器、电子邮件软件、工具软件等均不作为重要应用系统。

制定信息系统安全规划一方面要满足系统安全要求,并描述为满足系统安全要求所采取或应采取的安全控制方法；另一方面要明确所有对系统进行访问的人员的责任和行为规范。

安全规划设计过程中应在信息系统可承受的安全风险范围内,尽可能地考虑成本与效率,同时还要密切结合系统的安全要求及面临的威胁,制定科学、合理、可行的安全设计规划原则。总结各方面因素,进行安全方案设计、规划时应遵循以下几个原则：

1. 系统化

按照系统化的设计思想,在整合及综合考虑信息应用系统各个分系统安全需求的基础上,统一进行信息系统的安全设计规划,确保整个信息系统安全运行以及信息得到有效的安全保护。在网络基础设施方面,按分级分区的思想,统一规划、设计安全的系统网络环境,确保在网上传输的信息得到应有的保护,为各种网络应用的安全提供必要的支持。

2. 层次化

安全系统的规划设计,从应用系统层安全、网络层安全,到软硬件系统层安全,按层层防御的思想进行设计。每一层应实现所需要的安全功能,共同实现系统的整体安全。

3. 等级化

按照区域化保护的思想,根据信息系统不同域中的信息在存储、传输和处理过程中需要保护的程度,确定各个域所需要进行保护的安全等级,并明确划分每一个保护域的边界,按要求进行边界保护,防止来自外部的攻击和非授权访问,防止内部信息随意流出保护域,确保各个域中的信息得到应有的安全保护,确保各个域中的系统安全运行。

3.1.4 信息系统安全规划的作用

信息系统全面合理的安全规划是信息系统安全建设的基础和重要前提，对信息系统的整体架构及其安全体系具有良好的支持作用，同时也会显著提高系统所在组织的信息安全水平和管理能力。具体来说，信息系统安全规划有如下作用。

1. 系统运行集成化

- 降低和控制安全风险，提高信息系统的运行效率。
- 控制安全方面的投入成本，缩短信息系统安全体系建设周期。
- 提高系统相关人员的整体安全意识。

2. 安全管理流程合理化

- 系统整体安全性得到大幅度提升。
- 系统面对安全事件的响应速度大大加快。
- 系统用户满意度得到显著改善。

3. 系统安全监控动态化

信息系统可以根据安全管理需要，动态监控信息安全变化，以期实时地反馈和纠正安全管理中存在的问题。

4. 系统安全管理改善持续化

随着安全产品的应用和信息系统安全管理流程的合理化，系统信息安全管理水平将会明显提高。

3.1.5 信息系统安全规划的步骤

根据信息系统安全建设的体系化、层次化和等级化要求，结合系统本身的状况，设计整体的信息安全保障体系是安全规划的重要目标。

通过体系化，提出信息系统的安全建设目标和安全规划思路，建立总体安全体系和安全机制，从而保障信息系统的稳定、有效地运行，并帮助信息系统各级管理和操作人员明确具体安全要求，明确具体建设流程和维护步骤。

通过层次化和等级化，确定信息系统的安全等级和改造、建设的项目内容，确定系统安全保障设施的总体规模、安全保障策略和重点防护措施，并帮助领导决策安全投资规模，合理分配安全投资，准确把握投资重点。帮助信息系统的各级管理和操作人员确定重点工作和防范措施。

通过风险评估，从整体上掌握信息系统的安全建设情况，不仅是单纯的技术体系建设，同时要包括系统的信息安全管理、基础架构的运营与服务管理、业务分析和项目规划等。规划流程将从管理、技术和业务分析 3 个层面来描述其安全建设的方法和流程，具体如下：

安全体系规划路线分为规划准备、安全评估、规划设计、实施阶段、运行维护和优化完善 6 个环节，各个环节从管理、技术和业务等各个层面又存在不同的工作内容和安全要求。

1. 准备阶段

准备阶段的主要工作内容如表 3.1 所示。

表 3.1　规划思路——准备阶段工作内容表

实 现 层 次	工 作 内 容
管理	项目管理 项目计划
技术(基础架构的运营与服务管理)	运营技术战略
业务(业务分析、管理规范和项目规划)	业务需求分析 IT 战略分析 高级系统设计 业务案例的分析和政策 法规性符合分析

2. 评估阶段

评估阶段的主要工作内容如表 3.2 所示。

表 3.2　规划思路——评估阶段工作内容表

实 现 层 次	工 作 内 容
管理	安全架构分析 安全风险评估 安全技术现状评估
技术(基础架构的运营与服务管理)	运营现状分析 运营详细需求计划 网络可靠性评估 运营部署项目管理
业务(业务分析、管理规范和项目规划)	业务系统等级划分 详细需求计划 系统准备度分析 试点准备度分析 部署项目管理工作

3. 规划设计阶段

规划设计阶段的主要工作内容如表 3.3 所示。

表 3.3　规划思路——规划设计阶段工作内容表

实 现 层 次	工 作 内 容
管理	管理总体规划 安全策略与架构设计 安全实施设计
技术(基础架构的运营与服务管理)	技术总体规划 运营管理方案设计 运营管理实施方案 业务测试计划
业务(业务分析、管理规范和项目规划)	业务系统等级划分 详细需求计划 系统准备度分析 试点准备度分析 部署项目管理工作

4. 实施阶段

实施阶段的主要工作内容如表 3.4 所示。

表 3.4 规划思路——实施阶段工作内容表

实现层次	工作内容
管理	安全架构实施 安全制度与流程实施
技术(基础架构的运营与服务管理)	运营方案实施 业务准备度测试 运营培训
业务(业务分析、管理规范和项目规划)	试点实施 全局实施 迁移 试点准备度分析 系统接受性测试 培训

5. 运行维护阶段

运行维护阶段的主要工作内容如表 3.5 所示。

表 3.5 规划思路——运行维护阶段工作内容表

实现层次	工作内容
管理	安全审计 安全监控
技术(基础架构的运营与服务管理)	技术支持 硬件支持 软件支持
业务(业务分析、管理规范和项目规划)	资产管理 配置管理 系统监控与管理 变更管理

6. 优化完善阶段

优化完善阶段的主要工作内容如表 3.6 所示。

表 3.6 规划思路——优化完善阶段工作内容表

实现层次	工作内容
管理	安全巡检与审计 安全优化
技术(基础架构的运营与服务管理)	运营情况评估 运营优化
业务(业务分析、管理规范和项目规划)	业务案例评估 技术应用评估 技术优化

3.2　信息系统安全规划内容

随着信息化建设的高速发展以及信息系统本身对信息安全的高标准要求，使得统一安全规划和全面安全保障体系的建设成为必然。大型信息系统在建设安全系统时，不能像传统的安全系统那样，只有在出现漏洞时才进行安全补救，而应该系统地、有条理地进行全面综合的安全规划，充分地、全方位地考虑各种安全需求和特性，从而达到信息系统从软件到硬件，从计算模式到信息资源，从网络系统到安全管理，样样俱全、从里到外地充分得到保障。

信息系统安全规划的内容是根据安全规划的目标和原则要求以及各种安全需求和特性确定，主要包括对计算模式的安全规划、信息资源的安全规划、网络与系统的安全规划以及组织与管理的安全规划 4 个重要部分。

3.2.1　计算模式安全规划

计算模式是指组成计算机系统的各种硬件、网络、系统软件、应用软件等要素的逻辑和物理配置，是处于同一个网络中多台计算机共同工作的方式。

信息系统的计算模式大体分为 5 种：主机终端模式、文件服务器模式、客户机服务器模式(Client/Server，C/S)、浏览器服务器模式(Browser/Server，B/S)和云计算模式。现代信息系统的运行计算模式多为 C/S 模式和 B/S 模式。

1. 主机终端模式

主机终端模式是以大型机为中心(Mainframe-centric)的计算模式。在主机终端模式中，大型机的访问受到严格的控制，CPU 资源和数据存储同时由多个用户共享，数据通过简单的终端进行交换。在这种模式下，资源受到集中控制，用户界面不够友好，而且硬件投资巨大，如今已很少使用。

2. 文件服务器模式

文件服务器模式由客户机和文件服务器两部分组成，因此也被称为基于客户机的运行模式。在文件服务器模式下，文件服务器负责完成简单的工作，如保存共享数据以及应答客户机等，而客户机负责所有的数据处理。文件服务器模式实现了资源共享，并且具有简单易维护、实现成本低的优点。但在该模式下的文件数据传输不能够智能响应文件数据请求，造成网络中传输数据的大量冗余，还存在数据共享的加锁问题。因此，文件服务器模式仅仅适用于规模较小的局域网络，无法满足互联网中用户量多、数据量大的需求。

3. 客户机服务器模式

客户机服务器模式由客户应用程序和服务器管理程序组成。客户应用程序负责系统中用户与数据的交互，也称为前台服务系统。服务器管理程序的主要工作是高效地管理系统资源，当多个用户并发地请求服务器上的资源时，服务器管理程序负责对这些资源进行优化管理。C/S 模式具有以下几种优势：

(1) 交互性强。在 C/S 模式中，客户端应用程序非常完整，具有强大的在线帮助、出错

提示等功能，并且可以在子程序之间自由切换，具有很强的交互性。

（2）存取模式安全。C/S模式采用适用于局域网、安全性较好的网络协议，是配对的点对点的结构模式，能够提供更安全的存取模式。

（3）网络通信量低，处理速度快。C/S模式的网络采用两层结构，只包括客户端与服务器之间的通信量，这样能够降低网络通信量，提高处理大量信息的速度和能力。

由于C/S模式的上述优点，在20世纪末C/S模式便代替了主机终端模式和文件服务器模式。但随着Internet的不断普及和发展，C/S模式的局限性逐渐显露了出来。C/S模式的客户端过于庞大，导致应用程序的维护和升级工作量较大且成本很高。另外，C/S模式的事务层不能与跨平台的客户端共享，且没有统一的数据逻辑层来提供不同种类的数据存储。

4. 浏览器服务器模式

浏览器服务器模式以Web技术为基础，由一个数据服务器和多个应用服务器构成一个三层结构的客户服务器体系。第一层是用户与整个体系的接口，由一个通用的浏览器软件（如微软公司的IE浏览器）组成，浏览器为用户提供信息交互的平台，用户向浏览器网页提出处理信息的请求。第二层是Web服务器，负责响应用户请求，并将处理结果返回给客户机的浏览器。第三层是数据库服务器，负责管理数据库，并协调不同的Web服务器发出的请求。B/S模式具有以下优势：

（1）客户端简单灵活。在B/S模式下，无须在客户机上安装客户应用程序，而只需安装通用的浏览器软件。不但节省了客户机的硬盘空间与内存，而且使安装过程及网络结构更加灵活。

（2）易于开发和维护。系统开发者无须再为不同级别的用户设计开发不同的应用程序，只需根据不同的功能为各个级别的用户设置操作权限，再将所有的功能都实现在Web服务器上，从而简化了系统的开发和维护。

（3）用户操作简单。采用B/S模式时，客户端只是一个简单易用的浏览器软件，无论是决策层还是操作层的人员都无须培训，就可以直接使用。

（4）适用于网上信息发布，使得传统信息系统的功能有所扩展。

鉴于B/S模式相对于C/S模式的先进性，B/S模式逐渐成为一种流行的信息系统模式。当然，B/S模式并非没有缺点，一般来说，C/S模式的优点就是B/S模式的缺点，反之亦然。由于B/S模式的先进性和C/S模式的成熟性，很多应用信息系统实际上是将这两种模式结合在一起使用。

随着Internet和Web技术的发展，越来越多的企业开发基于B/S、C/S模式的信息管理系统，提高了信息管理的效率，减轻了手工操作的负担。B/S模式相对于C/S模式具有良好的跨平台性、易于维护和扩展等优点，但是随着信息量的膨胀，迎来严重的信息安全问题：非法或恶意的用户访问、数据的不一致、在公共网络上传输的数据被监控和修改等。因此在系统开发中建立一定的安全机制，增强系统的信息安全性，成为信息系统开发的一项重要内容，同时也是信息系统得以应用和延伸的基础。

B/S结构的信息系统一般由浏览器、Web服务器和数据库服务器组成，其安全规划涉及所用的操作系统、Web服务器、数据库系统和网络数据传输等。

（1）操作系统安全规划。

操作系统的安全是信息系统安全最基础的保证，一旦服务器的操作系统安全失效，其他

所有的安全将无法得到保证。只有正确地安装和设置操作系统，才能使其在安全方面发挥应有的作用。具体的安全策略如下：

- 正确地进行磁盘分区。
- 使用 NTFS 文件系统。
- 取消不必要的网络服务。
- 及时进行系统升级并安装补丁程序。
- 定期修改系统管理员口令。

（2）Web 服务器安全规划。

为了保证客户能够访问 Internet，Web 服务器必须与 Internet 连接，因此 Web 服务器的安全性要求很高。Microsoft Information Server（IIS）是一种 WWW 服务器，IIS 的设置可以确定用户访问服务器的方式以及用户所拥有的权限。Web 服务器的安全规划策略如下：

- 对 Web 应用程序设置正确的访问权限。
- 通过设置 IIS 用户的验证方式以及 IP 地址和网络域名来控制访问用户。
- 恰当地配置 Web 服务器，取消或删除不必要的服务。

（3）数据库安全规划。

数据库安全是保障数据的机密性、完整性和可用性，防止数据信息被非法窃取和篡改的有效措施。数据库系统的安全规划策略如下：

- 访问控制。通过用户名与密码体系对用户进行身份认证，保证只有具有访问权限的用户才能访问数据及网络资源，防止非授权用户的访问。
- 权限控制。根据最小特权和最大共享原则，用户只能在其权限范围内对数据进行操作，并为不同的数据库用户定义不同的操作权限。
- 数据库加密。用户采用自己的密钥对隐私信息进行加密，数据库管理员只能获得密文，而无法对其进行解密，从而保证了用户信息的机密性。
- 数据库备份。定期进行关键数据备份，保证数据库的可恢复性。

（4）数据传输安全规划。

目前数据传输对 Internet 的依赖越来越大，而 Internet 环境并不能够完全保证数据的安全通信，在传输过程中可能会发生数据窃取或篡改的状况，因此，需要制定相应的安全规划策略，来保证数据信息的安全传输。数据传输的安全规划策略如下：

- 使用 VPN 技术，为系统节点间的数据传输提供点到点的安全通道，提高数据传输的安全性和稳定性。
- 采用数据加密技术，对传输中的数据进行加密，并通过安全信道传输密钥信息，从而有效地保证数据传输的安全。

5. 云计算模式

随着云概念的提出，一种新的计算模式随之产生——云计算模式。云计算是由分布式计算、并行计算以及网格计算发展而来的新型计算模式。云计算体现了“网络就是计算机”的思想，将大量计算资源、存储资源与软件资源链接在一起，形成巨大规模的共享虚拟 IT 资源池（称为“云”），计算机可以通过“云”自动地管理和动态的分配与部署资源，从而为用户提供超大规模、虚拟化、安全可靠的服务。架构模式上的超前创新，使云计算模式在信息处

理和信息存储上具有非常显著的优势。

(1) 超强的运算能力。

云计算数据中心的规模决定了云计算信息处理能力。目前,谷歌云计算已经拥有100多万台数据处理服务器,而Amazon、IBM、微软等在云计算方面也都拥有几十万台服务器。而对于一般的企业而言,私有“云”的数量也都在成百上千台以上。强大的后台服务器能够赋予用户前所未有的计算能力。

(2) 可靠的信息服务。

云计算模式拥有用户规模庞大的“云”资源,对于每一个“云”而言,可以通过使用计算机节点同构可互换以及多副本容错技术等来保障信息服务的可靠性。

(3) 虚拟化的信息存储。

在云计算模式下,用户可以在任意位置通过互联网获取信息数据中心的应用服务。用户所请求的资源和数据均来自虚拟化的“云”数据中心。用户可以方便快捷地通过网络服务来实现所需要的一切,而不需要考虑内在的逻辑和计算过程。

(4) 较高的通用性和可扩展性。

云计算不针对特定的应用,在“云”的支撑下,可以构造出千变万化的应用,与此同时,云的规模也可以动态伸缩,满足应用和用户规模增长的需求。

(5) 按需服务的信息处理模式。

“云”是信息数据的支撑平台,“云”中存储着用户需要的所有数据和信息。因此,在云计算模式下,用户只要通过Internet连接云数据中心就可以按照需要进行信息的索取和计算。

云计算的自动化集中式管理使企业无须负担高昂的数据中心管理成本,云计算的通用性使资源的利用率大幅提升,用户可以充分享受云计算低成本的优势。但是,云计算模式下潜在的风险与威胁也不容忽视。云计算和其他的计算模式一样,存在一些共性安全问题和个性安全风险。

云计算的共性安全实质上是信息共享的安全,即信息存储和保密的程度。对于共性的安全问题,可以划分为4个层次。

(1) 设备安全。主要包括信息系统设备的稳定性、可靠性、可用性。

(2) 数据安全。针对“云”数据中心的数据,要保证其保密性、完整性、可用性。

(3) 内容安全。信息的真正价值体现在它的语意上,如果某条信息对用户而言其内容是无意义或没用的,那么所说的安全也没有价值。

(4) 使用安全。数据信息的使用安全主要包括信息使用行为的机密性、完整性和可控性。

云计算为数据处理和未来计算机发展提供了一种非常新颖的发展模式。在该模式下,除了共性安全性以外,对于用户而言还存在很多个性安全风险。首先,个性安全主要体现在云计算的服务特点上。云计算是以服务为中心的。这也就意味着云计算是面向大众、以人为本的,对专业领域数据加密能力不强。其次是可信性问题。如果云计算没有获得广大用户的信任,那么用户是不敢把数据存放到云环境中的。因此,云计算要做到既可靠又安全,广泛获取用户的信任,用户才会把数据存放于云数据中心。第三,系统的可靠性。防止数据丢失及失效,保障设备的稳定可靠运行都属于保障系统可靠性的范畴。因此,云计算系统应当具有抗灾容错的能力。第四,安全性。防止数据的泄密是数据的机密性问题,防止数据被

篡改是确保数据完整性的问题。

要想获得安全的云服务需要从技术、管理、外部审计、服务水平协议、法律法规等多个方面来构建全面的云应用防护体系。

3.2.2　信息资源安全规划

信息作为资源是马克卢普和波拉特等经济学家在 20 世纪 60 年代提出来的。如今信息资源作为国民经济的三大资源之一，其作用在当代社会与经济环境中越来越重要，所谓知识就是力量，知识就是财富，能否掌握信息资源就成为能否占据竞争优势的关键。信息系统是组织处理与利用信息资源的工具，信息资源作为信息系统的三大要素之一，信息系统安全规划的重点就是对信息资源的安全规划。

信息资源安全是指信息资源所涉及的硬件、软件及应用系统受到保护，以防范和抵御对信息资源不合法的使用和访问以及有意无意地泄露和破坏。信息资源安全包括了从信息的采集、传输、处理、存储和使用的全过程所涉及的安全问题。

从信息处理的角度，信息资源安全包括：

- 信息内容的真实无误，以保证信息的完整性。
- 信息不会被非法泄露和扩散，以保证信息的保密性。
- 信息的发送和接收者不可否认自己所做过的操作行为，以确保信息的不可否认性。

从信息组织层次的角度，信息资源安全包括：

- 系统的管理者对网络和信息系统有足够的控制和管理能力，以保证信息的可控制性。
- 准确跟踪实体运行达到审计和识别的目的，以保证信息的可计算性。
- 网络协议、操作系统和应用系统能够相互连接、协调运行，以保证信息的互操作性。

从信息运行环境角度，包括各种硬件设施的物理安全。从信息管理规范的角度，包括各种各样的规章制度、法律法规、人员安全性等。

威胁信息资源安全的主要因素包括：

(1) 非人为因素。

非人为因素是指不可控制的自然灾害，如地震、火灾、战争等，这种灾害轻则造成业务工作混乱，重则造成系统中断甚至造成无法估计的损失。

(2) 人为因素。

人为因素包括两种：“无意”因素和“有意”因素。“无意”因素是指人为的无意失误和各种各样的误操作等。典型的“无意”因素有操作人员误删文件，操作人员误输入数据，系统管理员为操作员的安全配置不当，用户口令选择不慎，操作人员将自己的账号随意转借他人或与别人共享等。“有意”因素指人为的对信息资源进行恶意破坏的行为。“有意”因素是目前信息资源所面临的最大威胁。“有意”因素主要包括以下 3 种类型。

① 恶意攻击：包括主动攻击和被动攻击两种形式。其中主动攻击是指以某种手段主动破坏信息的有效性和完整性；被动攻击则是在不影响信息(或网络)系统正常工作的情况下，截获、窃取、破译重要机密信息。这两种恶意攻击方式均可对信息资源造成极大的危害，并导致机密数据的泄露。

② 违纪：指内部工作人员违反工作规程和制度的行为。例如，银行系统的网络系统管

理员与操作员的口令一致，职责不分等。

③ 违法犯罪：包括制造和传播病毒、非法复制等，例如侵犯著作权、窃取机密、金融犯罪等。

(3) 信息系统自身的脆弱性。

计算机硬件系统的故障：因生产工艺或制造商的原因，计算机硬件系统本身存在故障，如电路短路、断路、接触不良等引起系统的不稳定、电压波动的干扰等。

软件的“后门”：指软件公司的程序设计人员为了自便而在开发时预留设置的，旨在为软件调试、进一步开发或远程维护提供方便。然而，这些软件的“后门”也为非法入侵提供了通道，一旦“后门”洞开，将会造成严重的后果。

软件的漏洞：软件不可能是百分之百无缺陷和无漏洞的，这些缺陷和漏洞往往是黑客攻击的首选目标，软件的错误(Bug)便是典型的漏洞。

由于信息系统中管理的是整个企业或单位的各种信息，其中往往还会有不少企业的机密信息，这就需要防止一些非授权用户“有意”或“无意”地获取这些信息。同时，在有些信息系统中，对系统中数据的不当操作也可能对企业或单位造成巨大的损失。此外，目前在网络中相当猖獗的计算机病毒，也可能会对网络信息系统产生难以预料的破坏。因此，必须采取有效的措施，保护网络信息系统中信息资源的安全。

对信息系统来说，信息资源保护的内容大致分为数据库级信息保护、服务器级信息保护、服务器代码级信息保护、客户端代码级信息保护等内容。

(1) 数据库级信息保护。网络信息系统绝大多数都要使用数据库，因此可利用数据库自身的安全特性和保密机制，来实现数据库的信息保护。如在 SIMMIS 中，使用了甲骨文公司的 Oracle 数据库。Oracle 的高级保密机制通过设置各种特权，控制对敏感数据的存取。用户根据连接到数据库的名称被赋予各种特权，如查看、修改和创建数据库等。用这些机制来保证只有授权用户才能查看敏感数据。另外，数据库都提供备份和恢复的功能。如 Oracle 提供了高级备份和恢复的子例程，能把数据丢失的可能性降到最小，并使出现故障时的排错时间最短。同时，Oracle 的服务器也提供了备份和恢复的机制，允许用户每天、每周、每年不间断地访问数据。

(2) 服务器级信息保护。网络信息系统的 Web 服务器(如 IBM 的 Websphere，Sun 的 Weblogic，Microsoft 的 IIS 等)，一般都具有安全和保护功能。在 SIMMIS 中，采取的 Microsoft 的 IIS 服务。对于在 Windows 操作系统的计算机上联网，IIS 是比较理想的，它可以在现有硬件上设置功能强大的 Web 服务器。IIS 利用了 Windows 的安全特征和性能优势，它在 Windows 操作系统上建立安全性模型，并提供附加监视和安全性保障。

(3) 服务器代码级信息保护。在网络信息系统中，可以充分利用编程语言的特性，编写各种各样的过程或函数，判断客户端浏览器所提交的请求是否合法。如在 SIMMIS 中，使用了 ASP 编程语言实现服务器代码级信息保护。

① 访问计算机的 IP 地址限制。在客户端对信息系统服务器端提交请求时，服务器端可以获得客户端的 IP 地址。因此，可以在代码中对客户端的 IP 地址进行判断，如果客户端的 IP 属于拒绝访问列表中的 IP 地址，那么服务器端将拒绝访问。

② 对访问某一页面的网址的限制。在网络信息系统中，可以从客户端请求中的 HTTP 报头得到客户端是由哪一个网页进入的。如果不希望用户只通过获知网址(URL)才可进

入,则可在程序中进行控制,规定只可由某几个链接点进入某一个网页。

③ 对访问某一页面的权限的限制。在网络信息系统中,由于每个用户的级别不同,他们对每个页面的权限也就不同。比如在学生成绩管理系统中,教师用户的权限是可以查看所有学生的成绩,而学生只能查看自己的成绩。因此可对某一个页面,设定其权限等级。在 SIMMIS 中,定义了“默认用户”、“注册用户”、“教师用户”、“领导用户”、“系统管理员”4 类用户,并设定了相应的权限。由于权限的不同,4 类用户所看见的页面也会不同,从而实现了信息系统的信息保护。

④ 高强度的加密系统。在网络信息系统中,为了防止黑客攻击或在请求传输过程中机密信息被泄露,可采取对信息加密的方法。在 SIMMIS 中,采用的是 SSL 加密系统。SSL 是提交给 W3C 工作组关于安全性的协议,它被视为 Internet 上 Web 浏览器和服务器的标准安全性措施。SSL 提供了用于启动 TCP/IP 链接的安全性“信号交换”,这种信号交换首先使客户和服务器同意使用的安全性级别,并履行链接的任何身份验证要求。此后,SSL 的唯一作用是加密和解密要使用的应用程序协议的字节流(如 HTTP)。这意味着 HTTP 请求和 HTTP 响应中的所有信息将完全被加密,包括客户正请求的 URL、任何提交形式的内容(如信用卡号)、任何 HTTP 访问身份验证信息(如用户名和密码)以及从服务器返回到客户的所有信息,从而实现了网络信息系统中信息传输过程的信息保护。

⑤ 访问超时控制。网络信息系统中使用访问超时限制。可以设置在一定的时间内如果没有接收到请求,服务器将自动结束这一访问状态。如果用户在浏览某站点的中途去做其他事情,如果时间已超过服务器认可的最长时间,则其访问会被自动关闭。

(4) 客户端代码级信息保护。在网络信息系统中,可以在客户端脚本中,使用各种各样的函数来验证客户端提交的请求,并在执行提交之前验证用户输入的内容是否为可接受的内容。如限制“年龄”输入框中的输入应该为日期的格式并大致在哪个年龄段之间,或者是验证“人数”输入框中的输入必须是正整数等。这样,可以有效地减轻服务器的某些工作,提高系统的效率。

在系统进行远程数据传输时,为防止数据泄露,可以采取密码措施进行保护。加密后,数据在传输过程中即使被入侵者截获,由于是密文形式,获取的信息也毫无价值。

3.2.3 网络与系统安全规划

目前计算机网络面临的风险及威胁越来越大,不仅面临黑客、竞争对手的威胁,心怀不满的员工也都有可能成为网络的潜在破坏者,为保障网络与系统的安全运行,一定要建立一套完整的防护体系。

一个全方位的计算机网络安全体系结构包含网络的物理安全、访问控制安全、系统安全、用户安全、信息加密、安全传输和管理安全等。只有充分利用各种先进的技术,如主机安全技术、身份认证技术、访问控制技术、密码技术、防火墙技术、网络反病毒技术、安全审计技术、安全管理技术、系统漏洞检测技术、黑客跟踪技术等,在攻击者和受保护的资源间建立多道严密的安全防线,才能够增加恶意攻击的难度及审核信息的数量,并且利用这些审核信息来跟踪入侵者。

网络的物理安全是整个系统安全的前提,网络的各项物理设施应符合国家有关安全保密标准。首先,系统所在的机房应满足防火、防水、防震、电力、布线、配电、温湿度、防雷、防

静电等方面的要求。其次,系统所用的安全保密产品原则上必须选用国产设备,并应获得国家保密工作部门批准。所用的非安全保密产品,优先选择国产设备,当需要选用国外设备时,应进行详细的调查与论证,必要时应对选用的国外产品进行安全保密检测。最后,系统中设备的安装使用应符合国家保密标准的要求,不符合要求的必须采取电磁泄漏的防护措施,如采取电磁屏蔽、线路传导干扰等措施,从而使得窃密者接收不到或还原不了信息。

为解决系统在运行层面的安全问题,应采取如防火墙、入侵检测、漏洞扫描、安全审计、身份鉴别、病毒防护等措施。防火墙的主要作用是在网络出口处检查网络通信情况,根据预先设定的安全规则,在保护内部网络安全的前提下,保障内外网络通信。在网络出口处安装防火墙(作为阻塞点、控制点),可有效地隔离内部网络与外部网络,提高内部网络的安全性。现在越来越多的蠕虫、病毒、木马和黑客能够成功突破防火墙对网络的保护,通过部署可与防火墙联动的入侵检测系统,实时分析进出系统的数据流,对攻击事件进行实时跟踪,及时发出安全警报并阻断攻击,从而使网络隐患降至最低限度。入侵检测设备可以置于防火墙前面,也可以置于防火墙后方。通过漏洞扫描系统的扫描分析,检查和报告系统网络设备、服务器主机、数据和用户账号及口令等所存在的安全风险、漏洞和威胁,及时采取补救措施与安全策略,配置或修改系统,从而达到增强系统安全性的目的。通过安全审计系统实时收集和监控系统中每个用户的每次活动(访问时间、地址、数据、程序、设备等)以及系统出错和配置修改信息,为系统管理人员审查用户提供依据,有助于提高信息系统安全管理的效率。建立身份鉴别机制,是保障信息系统安全的关键。对进入系统的用户身份进行认证,以判断该用户是否为系统的合法用户,通常采用口令方式或智能卡与口令相结合的方式进行身份鉴别。智能卡与口令相结合的方式安全性较高,且便于用户使用。日益泛滥的计算机病毒问题已成为信息安全的最严重威胁之一。计算机病毒一旦进入,传播难以控制,有可能迅速殃及整个系统,其破坏力和潜在的威胁是非常大的。因此,系统中应安装获得公安机关批准的防病毒软件,将杀毒软件的各种防病毒监控打开,进行全面监控,及时升级病毒库至最新版本,并定期查杀计算机病毒。

在实施网络安全防范措施时要考虑以下几点:加强主机本身的安全,做好安全配置,及时安装安全补丁程序,减少漏洞;要用各种系统漏洞检测软件定期对网络系统进行扫描分析,找出可能存在的安全隐患,并及时加以修补;从路由器到用户各级建立完善的访问控制措施,安装防火墙,加强授权管理和认证;利用数据存储技术加强数据备份和恢复措施;对敏感的设备和数据要建立必要的物理或逻辑隔离措施;对在公共网络上传输的敏感信息要进行数据加密;安装防病毒软件,加强内部网的整体防病毒措施;建立详细的安全审计日志,以便检测并跟踪入侵攻击等。

系统安全方面主要考虑操作系统安全和应用系统安全。选择操作系统时,尽量采用安全性较高的操作系统,并且对操作系统进行必要的安全设置,关闭一些不常用却存在安全隐患的应用。日常密切关注操作系统漏洞及补丁发布情况,争取在第一时间下载补丁,查漏补缺。

应用系统方面,不论是通用的应用软件,还是量身订制的应用软件,都存在安全风险。对于前者,参照加强操作系统安全的做法,及时发现、堵塞安全漏洞。对于后者,优选通过质量控制体系认证、富有行业软件开发经验的软件公司,加强软件开发质量控制,安排较长时间的试运行等策略,以规避风险,提高软件的防范水平。

3.2.4 组织与管理安全规划

信息系统的组织和管理安全是保证信息系统安全的有机整体，健全的信息系统安全管理组织是有效实施信息系统安全管理的前提，通过信息系统安全管理组织对信息系统进行安全的管理则是要达到的最终目的。

俗话说，“三分技术，七分管理”，组织与管理作为信息系统安全保障的重要组成部分，要保障系统稳健运行和信息安全，应该在以下几个方面采取措施。

1. 建立安全保密管理机构

健全信息系统安全管理组织机构，是保障信息系统安全的基础。一个健全的信息系统安全管理组织，应具有完善的机构设置和合理健全的管理规章制度，机构内工作人员各司其职、各尽其责、团结协作，确保各项安全工作顺利进行。建立安全保密管理机构，明确规定安全保密管理机构的职能。其具体职责是：制定系统安全保密管理制度和安全策略，包括技术策略和管理策略；制定并组织实施安全保密措施；定期进行信息系统安全保密检查。

2. 制定安全保密管理制度

信息系统安全与否很大程度上取决于具体的安全管理方法，许多用户为维护自身利益，在安全管理方法上做了大量的尝试，也积累了很多行之有效的经验，认真分析不难发现，实现安全管理的前提是严格的安全管理制度、明确的责任分工。认真严格执行并完善安全管理制度才能达到安全管理的最终目的。制定安全保密管理制度和系统安全策略，有利于加强系统运行管理，从而提高系统安全性、可靠性。

安全保密管理制度包括：物理环境与安全设施管理、设备和移动存储介质管理、计算机病毒与恶意代码防护管理、系统备份与恢复管理、系统运行与开发管理、系统安全审计管理、应急响应管理、内部人员管理、外部相关人员管理等。

系统安全策略包括：安全审计策略、备份与恢复策略、计算机病毒与恶意代码防护策略、身份鉴别策略、运行管理策略、系统安全性能检测策略、系统安全保密管理策略、信息完整性保护策略、应急响应策略等。

3. 配备系统管理人员

为保证系统的安全稳定运行，需要设置系统管理员、安全管理员和安全审计员等系统管理人员。系统管理员主要负责系统的日常运行维护工作，保证系统的正常运行。安全管理员主要负责系统的日常安全保密管理工作，包括用户账号管理、安全保密设备和系统所产生日志的审查分析。安全审计员主要负责对系统管理员、安全管理员的操作行为进行监督检查，并定期向系统安全管理机构汇报相关情况。

4. 使用用户权限管理策略

通常信息系统都包含许多相对独立的应用子系统，为了避免各子系统单独使用自己的权限管理系统，导致重复开发、权限管理分散等问题，考虑将系统访问权限管理也独立出来，对权限进行集中管理。目前，基于角色的访问控制（RBAC）技术已比较成熟，其核心思想就是将访问权限与角色相联系，通过给用户分配合适的角色，让用户与访问权限相联系。根据用户在企业中的职责来设定用户的角色。用户可以在角色间进行转换，系统可以添加、删除角色，还可以对角色的权限进行添加、删除。这样通过应用 RBAC 将权限管理变成类似于

企业日常的组织管理。

在 RBAC 中，角色作为一个桥梁沟通于用户和资源之间。对用户的访问授权转变为对角色的授权，然后再将用户与特定的角色联系起来。权限被授予给角色，角色被授予给用户，用户不直接与权限相关联。用户只有通过角色才享有该角色所对应的权限，从而访问相应的客体。角色的权限即为角色所拥有的功能，表现为对某一子系统或一系列菜单项可执行功能，称为功能项。一旦一个 RBAC 系统建立起来以后，主要的管理工作即为对角色授权或更改用户的角色。

5. 加强人员管理

人是具有复杂情感的动物，要做好人员管理并不是一件容易的事情。但在信息系统安全管理中，人员管理占据举足轻重的地位，要加大管理力度，使人员管理在信息系统安全中发挥应有的作用。

人员管理包括内部人员和外部相关人员管理。

1）内部人员管理

系统内的管理人员和操作使用人员也是信息安全隐患的一个重要因素。首先要对人员的个人经历、社会关系、政治思想状况、职业道德等进行审查，确保系统中每个用户都安全可靠。其次，明确岗位职责，使每个用户都能够按照自己的岗位和职权使用系统。

除加强对系统管理人员及操作使用人员进行计算机技术及使用操作培训外，还要重点培训系统使用方面的安全操作知识，包括登录、退出等基本操作规范以及口令保密意识等。同时对系统管理员，还要做更深入的技术培训，如系统的运行维护、非法入侵的识别能力与防范能力等。

2）外部相关人员管理

外部相关人员是指经常或一段时间内需要进入系统现场进行维修、服务的外部人员。应采取相应的技术和管理手段，加强外部相关人员的管理，具体包括保密要求、安全控制区域隔离、携带物品限制和旁站陪同控制等四个方面。

3.3 信息系统安全规划模型与方法

信息系统安全规划模型与方法是保证安全系统的有效手段，在安全规划过程中选择适当的安全模型与方法，将起到事半功倍的作用。本节在探讨现有信息系统安全模型的基础上，分析了访问控制模型和信息流模型的优缺点；并针对信息系统安全的实际要求，对安全模型进行了改进；最后根据安全系统设计的原则，提出了信息系统安全规划的总体实现方法。

3.3.1 安全规划模型

随着 Internet/Intranet 技术的迅速发展和广泛应用，信息系统的安全，特别是网络系统的安全逐渐成为人们日益关注的问题。所谓信息系统安全是指机密性、有效性、真实性、完整性和信息可用性的结合。为了有效地保护信息安全，人们开发出多种信息安全技术，但理论上不存在绝对安全的系统。设计出一个优越的安全系统的关键是提出并实现详尽全面的安全策略，即要对系统的安全需求分析以及安全控制方法有一个清晰、全面的理解和描述。

安全模型就是安全策略的一种精确描述,它在安全系统开发中起着关键的作用。最早的安全模型是用于描述军事安全策略的,随着计算机的迅速普及,适用于各种应用领域安全需求的安全模型不断被提出。安全模型具有下列特点:

(1) 它是精确的,无歧义的。

(2) 它是简单和抽象的,容易理解。

(3) 它是一般性的,只涉及安全性质,不过度地抑制系统的功能及实现。

信息系统安全的最终目标是保障信息的保密性和完整性,因此从这一点来分析,信息系统的安全规划模型应该主要针对这两点。图 3.1 表示的是安全模型与安全目标的关系。



图 3.1　安全模型与安全目标的关系图

由图 3.1 可知,保障信息系统的保密性的模型分为两种:一种是访问控制模型;另一种是信息流模型。

1. 访问控制模型

访问控制是确保信息系统安全的重要措施之一。访问控制模型是从访问控制的角度描述安全系统,主要针对系统中主体对客体的访问及其安全控制。访问控制安全模型中一般包括主体、客体,以及为识别和验证这些实体的子系统和控制实体间访问的参考监视器。通常访问控制可以分为自主访问控制、强制访问控制以及基于角色的访问控制 3 类。

1) 自主访问控制(Discretionary Access Control,DAC)

自主访问控制是一种最普遍的访问控制策略,DAC 中主体对客体的访问权限是由客体的拥有者所决定的,也就是说,系统允许客体的拥有者可以按照自己的意愿自主地将该客体的访问权限或访问权限子集授予其他主体。

2) 强制访问控制(Mandatory Access Control,MAC)

系统给主体和客体分配不同的安全属性,在实施访问时,系统须对主体和客体的安全属性进行比较,再决定主体能否访问客体。强制访问控制对主体和客体标记两个安全标记:一个是具有偏序关系的安全等级标记;另一个是非等级分类标记。强制访问控制的另一个特征是不能“向下写”信息,也就是说在系统中不允许向下一级泄密。军方一直使用信息安全等级和范畴的方法来保证信息的授权访问。

MAC 通过分级的安全标签实现了信息的单向流通,其中最著名的是 Bell-LaPadula 模型。Bell-LaPadula 模型具有只允许向下读、向上写的特点,可以有效地防止机密信息向下级泄露。

下面对 MAC 模型中的两种主要模型进行介绍：

(1) Bell-LaPadula(BLP)模型。

1973 年，D. E. Bell 和 L. J. LaPadula 提出了一个可证明的安全系统模型，就是 Bell-LaPadula 模型，简称 BLP 模型。在随后的几年中，BLP 模型得到了进一步的充实和改善。Bell 和 LaPadula 在 1976 年完成的研究报告中给出了 BLP 模型最完整的表达，其中包含模型的形式化描述和非形式化说明。

BLP 模型是典型的信息保密性多级安全模型，主要应用于军事系统。BLP 模型通常是处理多级安全信息系统的设计基础，客体在处理绝密级数据和秘密级数据时，要防止处理绝密级数据的程序把信息泄露给处理秘密级数据的程序。BLP 模型的出发点是维护系统的机密性，有效地防止信息泄露。

BLP 模型是一个状态机模型，它定义的系统包含一个初始状态 z_0 和由一些三元组(请求，判定，状态)组成的序列，三元组序列中相邻状态之间满足某种特定的关系 W。如果一个系统的初始状态是安全的，并且三元组中所有状态都是安全的，那么这样的一个系统就是安全的。

在 BLP 模型中，系统状态用四元组(b,M,f,H)来表示，其中 b 表示当前访问集合；M 是访问控制矩阵；f 代表安全等级函数，用于确定任意主体和客体的安全等级；H 表示客体层次关系。当前访问可用三元组(S,O,x)表示，其中 S 是主体(Subject)，指用户、进程等主动实体；O 是客体(Object)，指文件等受主体控制的实体；x 是访问权限，包括 r(只可读)、a(只可写)、e(可执行)、w(可读写)4 类。主体的安全级别包括最大安全级别和当前安全级别，最大安全级通常简称为安全级别。

BLP 模型是一个多级安全模型，多级安全(Multilevel Security，MLS)的核心思想是防止高密级的信息泄露给低密级的主体，为了形式化地描述 MLS 策略，假设系统中客体 O 的安全级为 Level(O)，主体 S 的安全级为 Level(S)，当前的一个系统状态表示为 State_t，则 MLS 可以形式化描述为：对任意非可信主体 S，若 $(S,O_1,r)\in b_t$，$(S,O_2,a)\in b_t$，则 $\text{Level}(O_1)\leqslant\text{Level}(O_2)$。这里的 b_t 表示状态 State_t 中的当前访问集合，$(S,O,x)\in b_t$ 表示 b_t 中允许主体 S 以方式 x 访问客体 O。BLP 模型通过以下两条安全属性实现了 MLS 策略。

① 简单安全属性：当且仅当主体的安全等级大于等于客体的安全等级时，才允许主体对客体进行读操作，即如果 $(S,O,r)\in b_t$，则 $\text{Level}(O)\leqslant\text{Level}(S)$。

② *-属性：当且仅当主体的安全等级小于等于客体的安全等级时，才允许主体对客体进行写操作，即如果 $(S,O,a)\in b_t$，则 $\text{Level}(O)\geqslant\text{Level}(S)$。

简单安全属性禁止低安全等级的主体对高安全等级的客体的读访问(即“向上读”)，而 *-属性则禁止高安全等级的主体向低安全等级的客体写入信息(即“向下写”)，这两个属性构成了 BLP 模型的强制存取控制策略。

尽管 BLP 模型能够很好地防止信息的非授权泄露，保护信息的机密性，但它仍存在一些不足：

① 由于“盲写”引发的信息完整性问题。

BLP 模型只是为了适应军事和政府部门计算机系统的安全需要，可以有效地防止信息

的非授权访问和特洛伊木马的攻击，但由于不允许"向上读"，只能够"向上写"，即所谓的"盲写"，容易引发信息的完整性问题。

② BLP 模型缺乏对可信主体访问权限的限制。

Bell 指出用 *-属性限制所有主体的系统是不实用的。为了保障系统的有效运行，不得不存在一些违反模型中 *-属性的操作，例如，高安全级的主体向低安全级的主体传递非密级消息，系统通过定义可绕过 *-属性检查的可信主体（Trusted Subject）来实现。这一设计导致可信主体可以绕过 BLP 模型的 *-安全属性的限制，其行为完全在 BLP 模型的控制之外，后来很多人对其进行了改进，本质上都是为可信主体设定一个安全级范围，从而使可信主体只是部分可信。

③ BLP 模型的安全性依赖于安全平稳性规则，即主客体的安全级在整个生命周期中不可变。严格执行平稳性原则在保障模型安全性的同时，也造成了对非可信主体的限制过强，限制了 BLP 模型的实用性和灵活性。

根据 BLP 模型的不足之处，后人提出了多种改进 BLP 模型的方式与方法。大体的改进思路分两个方面：一方面是从信息的完整性角度改进；另一方面是通过一定的强制规则在保持模型安全性的前提下实现对主体安全级别的动态调节，从而能够更好地满足实际应用的需求。

（2）Chinese Wall 模型。

Chinese Wall 模型主要解决商业中的利益冲突问题。它假定系统数据按信息个体项、数据集合利益冲突类的组织形式存放，并将这些数据分为脱敏数据和未脱敏数据。

设 COI(o)表示包含客体 o 的 COI 类，CD(o)表示包含客体 o 的数据集，PR(s)表示主体 s 曾经读取过客体集合，并假设每个客体只属于某个 COI 类，则 Chinese Wall 模型的安全规则如下：

① 简单安全规则。

主体 s 可以对客体 o 执行读操作，当且仅当以下条件之一成立：

- 存在一个客体 $o'\in \mathrm{PR}(s)$，且 $\mathrm{CD}(o')=\mathrm{CD}(o)$。
- 对于所有客体 o'，$o'\in \mathrm{PR}(s)\Rightarrow \mathrm{COI}(o')\neq \mathrm{CD}(o)$。
- 客体 o 是脱敏的。

② *-特性。

主体 s 可以对客体 o 执行写操作，当且仅当以下条件都成立：

- 简单安全规则允许 s 对 o 执行读操作。
- 对所有未脱敏客体 o'，s 可以读 $\mathrm{CD}(o')=\mathrm{CD}(o)$。

3）基于角色的访问控制（Role-Based Access Control，RBAC）

RBAC 的核心思想是引入角色的概念，将操作权限直接授予角色而非用户，用户通过角色身份来获得相应的操作权限。这种访问控制方法特别适合于同一个职务由多个成员来担任的应用场合。例如，一个医院的外科医生、内科医生和儿科医生等都必须有多个才能满足大量患者的看病需求。因此，在医疗系统中可以定义外科医生、内科医生和儿科医生等各种角色，在外科医生中又可细分为普通外科、胸外科和脑外科等，对此，在 RBAC 中，可用子角色的方式来控制其权限。又例如，在一个大型的办公系统中，由于来往的文件数量巨大，可能需要有多个文件收发员负责对外的文件收发工作，也需要有多个文秘人员负责文件的处

理,如根据文件的来源单位和内容送给相关的部门和领导批阅,也需要有多个档案管理人员对处理完的文件进行归档保存,在这种情形下,便可在系统中设置文件收发员、文秘人员和归档人员等各种角色,赋予这些角色中的成员相同的操作权限。

基于角色的授权方法相对于对单个用户授权,大大地简化了授权的机制和管理,在用户的工作职务发生变化时,只要转换他的角色身份,而不需要对其进行重新授权;当机构设置发生变化时,如某个部门撤销、某些部门合并等,也可以不修改应用程序,而只要修改角色与用户、角色与操作权限之间的配置关系即可。

在基于角色的访问控制系统中,当用户初次进入系统时,系统根据用户的职务(或工作职责)为其分配相应的角色,从而让其取得这些角色的访问权限。但在系统运行的过程中,用户可能需要从一个角色转换成另一个角色。例如,职务升迁或工作调动;也可能在某些情况下,用户需要将自己的工作委托给另一个用户来完成,例如出差、生病等。系统可用授权机制来满足这类需求。

这里的"授权"是指拥有某角色的用户将该角色的成员资格授予其他用户。根据实际需要,授权可以采取各种方式,下面列出了授权的几种特征。

(1) 永久性:指授权有效期的长短,分为永久授权和暂时授权两种类型。永久性授权是指被授权用户永久地取得了被授予的角色成员资格。暂时授权是指被授权用户只在一段时间内得到被授予的角色成员资格,一旦有效期结束,这种授权也就被回收。

(2) 同一性:指授权者授权后,自身是否还拥有角色的成员资格。同一性授权后,授权用户仍拥有原角色的成员资格。非同一性授权后,授权用户丧失了原角色的成员资格,直到授权回收,再重获原角色的所有权限。

(3) 全部性:指是否授予角色的全部权限。全部性授权的授权用户将角色的所有权限授予被授权用户。在这种情形下,角色的成员用户可分为两类:原始成员和被授权成员。前者是系统安全员最初分配到角色中的成员,后者是由该角色中的成员通过其授权分配到角色中的成员。部分授权的被授权用户只被授予角色的部分权限。

(4) 执行性:指授权由谁执行。自主执行是由授权者本人执行,代理执行是授权者向第三方(某个代理)提出请求,让其完成自己的授权,但代理者不能给自己授权。

(5) 传递性:指被授权用户能否将角色成员资格转授出去。单步授权时被授权者不能将得到的角色再转授给其他用户,这意味着角色中的被授权成员无权将该角色的权限转授出去。多步授权的角色成员资格可以像接力棒一样,被传来传去。

(6) 多重性:指授权者在同一时刻可以对多个用户授权。

(7) 协议性:指授权是否要征得被授权者同意。确认协议授权必须有双方都认可的协议,以确保授权方与被授权方都同意此次授权。非确认授权不需要被授权者的认可,一旦授权者发出授权,被授权者必须接受。

关于授权回收可以有以下几种策略。

- 基于支撑角色的回收:若某个用户是在角色 A 的背景下,取得了角色 B 的授权,则当角色 A 的授权被回收后,角色 B 的授权也被回收。
- 基于发起角色的回收:若用户甲对用户乙进行了某角色的授权,当用户甲的角色被回收之后,用户乙也不能拥有该角色。

- 授权者有关回收：只有授出权限的用户才能回收他所授出的权限，角色中的任何其他成员均无权回收。

上述授权机制体现了用户的自主性，它与传统的自主访问控制相比，其授权不是基于权限而是基于角色，所以简化了系统对授权的管理，也更适合于实际系统的应用需求。

在大型系统中，角色数可能是成百上千，而用户数则可能是成千上万，对这些角色和用户的管理是一项非常复杂的工作，它不可能由一个系统安全员去完成。下放 RBAC 的管理权，而又不失广义上的集中式控制的 ARBAC97 模型，给出了如何基于 RBAC 来实现对角色和用户的管理。

由前面的介绍可以看出，RBAC 是中性的策略。它实际上是提供了一种描述安全策略的方法或框架。通过对 RBAC 各个部件的配置，以及不同配件之间进行交互的方式，可以在很大的范围内实现所需要的安全策略。

例如，通过基于角色的授权方式可以实现自主访问控制，而且比传统的自主访问控制更为灵活和方便。通过角色—用户的配置及角色—权限的配置可以实现系统所需要的各种强制访问控制策略。若采用 RBAC1 模型建立角色层次关系，则可实现多级安全的控制策略。RBAC2 的约束机制为实现强制访问控制提供了更为丰富的手段。在 RBAC 的角色—用户配置中最极端的情形是，一个角色仅具有一个用户，这时便可等同地实现传统的自主访问控制和多级安全控制策略。

为适应系统需求的变化而改变策略的能力也是 RBAC 的一个重要的优点。当应用系统增加新的应用或新的子系统时，RBAC 可以赋予角色新的访问权限，可以为用户重新分配一个新的角色，同时也可以根据需要回收用户的角色身份或回收角色的权限。

RBAC 支持以下 3 条安全原则：

(1) 最小特权原则。

RBAC 可以使分配给角色的权限不超过具有该角色身份的用户完成其工作任务所必需的权限。用户访问某资源时，如果其操作不在用户当前被激活角色的授权范围之内，则访问将被拒绝。

(2) 职责分散原则。

RBAC 可以对互斥角色的用户进行限制，使得没有一个用户同时是互斥角色中的成员，并通过激活相互制约的角色共同完成一些机密的任务，以减少完成任务过程中的欺诈行为。

(3) 数据抽象原则。

在 RBAC 中不仅可以将访问权限定义为操作系统(或数据库)中的读或写，也可以在应用层上定义权限，如存款和贷款等抽象权限。支持数据抽象的程度将由实施细节决定。

RBAC 引入了角色的概念，通过角色与用户、角色与权限的配置为系统实现其安全控制提供了灵活且强有力的保护。这种保护可适用于多种不同的安全需求，而不仅限于多级安全。在计算机应用日益广泛，各种应用的安全需求呈现多样化的形势下，特别是对于金融、商业和大型企业的安全控制，RBAC 提供了一种理想和实用的模式，因此，RBAC96 模型簇提出后，便受到信息安全特别是访问控制专家的广泛关注和热烈讨论，并进一步探讨了 RBAC 在多域访问控制中的应用。

2. 信息流模型

信息流模型主要着眼于对客体之间的信息传输过程的控制，通过对信息流向的分析可

以发现系统中存在的隐蔽通道,并设法予以堵塞。信息流是信息根据某种因果关系(例如函数)的流动,信息流总是从旧状态的变量流向新状态的变量。信息流模型的出发点是彻底切断系统中信息流的隐蔽通道,防止对信息的窃取。隐蔽通道就是指系统中非正常使用的、不受强制访问控制正规保护的通信方式(例如存储信道和定时信道)。隐蔽通道的存在显然危及到系统敏感信息的保护。

信息流模型需要遵守的安全规则是:在系统状态转换时,信息流只能从访问级别低的状态流向访问级别高的状态。信息流模型实现的关键在于对系统的描述,即对模型进行彻底的信息流分析,找出所有的信息流,并根据信息流安全规则判断其是否为异常流。若是就反复修改系统的描述或模型,直到所有的信息流都不是异常流为止。

信息流模型是一种基于事件或踪迹的模型,其焦点是系统用户可见的行为。在信息流安全系统中,对于信息流安全来说这是一种可以俘获所希望俘获的信息的直观方法。现有可用的信息流模型定义了什么是所期望的外部可见行为,但并没有直接指出哪种内部信息流是被允许的以及哪种是不被允许的。尽管信息流模型对安全系统有一个简单而且漂亮的定义,但是,安全性的输入输出规范对于在实际系统中的实现和验证并没有太大的帮助和指导,所以正如 John McLean 曾经指出的那样,这些把焦点放在系统用户的可见行为上的安全模型不能对内部具有因果限制关系的保密性要求进行很好的建模。尽管对于这种内部的保密性要求,已经有人提出了另一种基于计算状态的形式化模型,它们对信息流中的内部限制提供了更好的理解,但是迄今为止,信息流模型对具体的实现只能提供较少的帮助和指导。

根据图 3.1,保障信息系统完整性的模型有两种:Biba 模型和 Clark-Wilson 模型。

1) Biba 模型

Biba 模型是人们在研究 BLP 模型的特性时发现的,BLP 模型实现了信息的保密性,但在信息完整性方面存在一些缺陷,没有采取有效的措施来制约用户对信息的非授权修改,因此使非法、越权篡改成为可能。考虑到上述因素,Biba 模型模仿 BLP 模型的信息保密性级别,定义了信息完整性级别,用户只能向比自己安全级别低的客体写入信息,从而防止非法用户创建安全级别高的客体信息,避免越权、篡改等行为的发生。

Biba 模型禁止"向上写",完整性级别高的文件只能由完整性高的进程创建,从而保证完整性级别高的文件不会被级别低的文件所覆盖。Biba 模型没有"向下读"。

Biba 模型的偏序关系可以表示为:

(1) ru,当且仅当 $SC(s) \leqslant SC(o)$,允许读操作。

(2) wd,当且仅当 $SC(s) \geqslant SC(o)$,允许写操作。

Biba 模型是和 BLP 模型相对立的模型,Biba 模型改正了被 BLP 模型所忽略的信息完整性问题,但在一定程度上却忽视了保密性。

在 Biba 模型中各个元素的数学定义如下:

S——主体 s 的集合,系统中主动的信息处理元素。

O——客体 o 的集合,系统中被动的信息储存元素。

S 与 O 的交集为空集。

I——完整性级别的集合。

II——$S \times O \Rightarrow I$,定义每一个主体和客体完整性级别的函数,定义在关系 leq 下的一个

网格。

leq——定义在完整性级别 I 集合中的“小于等于”关系（$I \times I$ 的子集）。

min——POWERSET(I)$\Rightarrow I$，返回 I 的子集的最大低限的函数。

o——定义主体能力的关系（$S \times O$ 的子集），S 的元素 s 观察一个客体 o：$s\ o\ o$。

m——定义主体能力的关系（$S \times O$ 的子集），S 的元素 s 修改一个客体 o：$s\ m\ o$。

i——定义主体能力的关系（$S \times O$ 的子集），S 的元素 s_1 调用另一个主体 S 的元素 s_2：$s_1\ i\ s_2$。

子系统是一个系统的主体和客体可能基于功能或权限被隔离的子集，一个计算机系统可以定义为由一个以上的子系统所组成。在 Biba 模型中，将完整性威胁分为来源于子系统内部或外部两种。如果子系统的一个组件是恶意的或不正确的，则将产生内部威胁；如果一个子系统企图通过提供错误数据或不正确调用函数来修改另一个子系统，则将产生外部威胁。由于内部威胁可以通过程序测试或检验来有效解决，所以 Biba 模型仅仅针对外部威胁。

Biba 模型支持 5 种不同的完整性策略，即最低点策略、针对客体的最低点策略、最低点完整性审计策略、Ring 策略和严格的完整性策略。

(1) 最低点(Low-Water Mark)策略。

在该策略中，一个主体的完整性级别不是静态的，而是一个以以往行为为依据的函数。策略对每个主体提供 il(s)的动态的、单一的且不增长的值。在任何时刻，il(s)的值都反映了主体以往行为的最低点，最低点是被主体当作“观察”访问的客体的最小完整性级别，可以用以下公理描述。

对于 S 的所有 s 元素和 O 的所有 o 元素：

$$s\ m\ o \Rightarrow \mathrm{il}(o)\ \mathrm{leq}\ \mathrm{il}(s)$$

对于 S 的所有 s_1 和 s_2 元素：

$$s_1\ i\ s_2 \Rightarrow \mathrm{il}(s_2)\ \mathrm{leq}\ \mathrm{il}(s_1)$$

对于主体 s 对客体 o 的每一次观察访问：

$$\mathrm{il}'(s) = \min\{\mathrm{il}(s), \mathrm{il}(o)\}$$

(2) 针对客体的最低点策略。

针对客体的最低点策略除了修改主体的完整性级别外，还假设客体的完整性级别也被修改。可以用下列规则来说明。

对于一个主体 s 对一个客体 o 的每一次观察访问：

$$\mathrm{il}'(s) = \min\{\mathrm{il}(s), \mathrm{il}(o)\}$$

对于一个主体 s 对一个客体 o 的每一次修改访问：

$$\mathrm{il}'(o) = \min\{\mathrm{il}(s), \mathrm{il}(o)\}$$

(3) 最低点完整性审计策略。

审计策略是对于客体的最低点策略的非强制性的变化，它对较低完整性级别的信息对数据的可能损坏提供度量。

可以用下列方法来定义主体和客体的“当前损坏程度(Current Corruption Level，cl)”。

对于一个主体 s 对一个客体 o 的每一次观察访问：

$$\mathrm{cl}'(s) = \min\{\mathrm{cl}(s), \mathrm{cl}(o)\}$$

对于一个主体 s 对一个客体 o 的每一次修改访问：

$$\mathrm{cl}'(o) = \min\{\mathrm{cl}(s), \mathrm{cl}(o)\}$$

对于一个客体而言，cl 的值表示可以被用来修改客体的信息的最小完整性级别。

(4) Ring 策略。

Ring 策略为直接修改提供保护策略。主体和客体的完整性级别在其生命周期中是固定的，而且只允许小于等于客体完整性级别的修改。系统的灵活性通过允许在任何完整性级别上对客体的观察而显著增强。

该策略由以下两条公理定义。

对于 S 的所有 s 元素和 O 的所有 o 元素：

$$s\ m\ o \Rightarrow \mathrm{il}(o)\ \mathrm{leq}\ \mathrm{il}(s)$$

对于 S 的所有 s_1 和 s_2 元素：

$$s_1\ i\ s_2 \Rightarrow \mathrm{il}(s_2)\ \mathrm{leq}\ \mathrm{il}(s_1)$$

(5) 严格完整性策略。

该策略由 3 部分组成：简单完整性条件、完整性 *-属性和调用属性。

① 简单完整性条件。

规定一个主体不能观察具有较低完整性级别的客体，用数学方法表示如下。

对于 S 的所有 s 元素和 O 的所有 o 元素：

$$s\ o\ o \Rightarrow \mathrm{il}(s)\ \mathrm{leq}\ \mathrm{il}(o)$$

该规则限制了客体(数据或程序)对那些非恶意字符(取决于它们的完整性级别)的使用。Biba 模型认为"执行"访问等于"观察"访问，所以客体的完整性级别必须大于等于发出"执行"请求的主体。

② 完整性 *-属性。

规定一个主体不能修改具有较高完整性级别的客体，用数学方法表示如下。

对于 S 的所有 s 元素和 O 的所有 o 元素：

$$s\ m\ o \Rightarrow \mathrm{il}(o)\ \mathrm{leq}\ \mathrm{il}(s)$$

该规则保证了客体不能被权限不足的主体直接修改。

③ 调用属性。

规定一个主体不能向具有较高完整性级别的主体发送信息。用数学方法可描述为接收信息的主体的完整性级别必须小于等于发送信息的主体的完整性级别。

对于 S 的所有 s_1 和 s_2 元素：

$$s_1\ i\ s_2 \Rightarrow \mathrm{il}(s_2)\ \mathrm{leq}\ \mathrm{il}(s_1)$$

调用是从一个主体到另一个主体的逻辑请求服务。由于被调用主体的控制状态是主体被调用事实的函数，调用是修改的一个特例，所以，该规则直接跟随完整性 *-属性。

Biba 模型定义的完整性只是一个相对的而不是绝对的度量。依据该定义，一个子系统拥有完整性属性的条件是它可被信任并附着一个定义明确的行为代码。没有一个关于该行为属性的描述语句来决定子系统是否拥有完整性，所以需要子系统附着行为代码。

对于 Biba 模型而言，计算机系统完整性的目的是确保子系统完成设计者预期的目标。但现实的情况是，设计者是否采用了可以达到完整性的设计方法。

Biba 模型用一个结构化网格来表示授权用户和提供用户类型级别的划分。这些属性

可以防止非授权用户的修改。

到目前为止，在所有 Biba 模型的策略中，使用最广的是严格完整性策略。该策略的缺点是不能分配适当的完整性标志。BLP 模型能很好地满足政府和军事机构关于信息分级的需求，Biba 模型却没有决定完整性级别和类别的相应标准。

2）Clark-Wilson 模型

（1）模型的定义。

Clark-Wilson 完整性策略模型是由克拉克（D. D. Clark）和威尔逊（D. R. Wilson）提出的保护数据完整性的访问控制策略，简称 C-W 模型。C-W 模型是一个面向事务（Transaction）的模型，事务是操作的集合，一个事务由一组操作构成。事务作用在数据上，该模型的出发点是确保数据和事务的完整性。

定义 1　如果一个事务使系统从一个有效状态转换到另一个有效状态，则这样的事务称为良构事务（Well-formed Transaction）。

C-W 模型针对事务在数据上的作用建立完整性控制的体系架构，它把系统中的所有事务划分为两大类：约束数据项和非约束数据项。

定义 2　在一个系统中，处于完整性模型的控制范围之内的数据项称为约束数据项（Constrained Data Item，CDI），处于完整性模型的控制范围之外的数据项称为非约束数据项（Unconstrained Data Item，UDI）。

C-W 模型把所有 CDI 都满足完整性策略要求时的系统状态定义为有效状态，与状态相关，C-W 模型定义了两类事务：完整性验证过程和转换过程。

定义 3　在 C-W 模型中，用于验证系统是否处于有效状态的事务称为完整性验证过程（Integrity Verification Procedure，IVP），用于使系统从一个有效状态转换到另一个有效状态的事务称为转换过程（Transformation Procedure，TP）。

根据有效状态的定义，在有效状态下，CDI 的完整性是有保障的，要确保 CDI 的完整性就是要确保系统处于有效状态。

C-W 模型实现完整性控制的基本思想是：假设系统在某个初始时刻处于有效状态，在系统运行过程中，模型确保只有 TP 能够对 CDI 进行操作，进而确保只有 TP 能够改变系统的状态。

由于 C-W 模型要实现的 TP 是良构事务，所以系统在运行过程中总是处于有效状态，因而系统的完整性可以得到保障。

（2）模型的规则。

系统可以实现 TP，也可以确保只有 TP 能够对 CDI 进行操作，但系统本身无法确保 TP 是良构事务。

C-W 模型采取两类措施实现系统的完整性：一类是由系统实施的措施；另一类是证明系统实施有效性的措施。与此相对应，C-W 模型定义两类规则：实施规则和证明规则。

定义 4　在 C-W 模型中，由系统实施的规则称为实施（Enforcement）规则，简记 E 规则；用于证明系统实施规则有效性的规则称为证明（Certification）规则，简记 C 规则。

以下规则构成了 C-W 模型的基础框架，它确保 CDI 的内部一致性。

规则 C1　IVP 必须验证所有的 CDI 在 IVP 运行时刻都处于有效状态。

规则 C2　必须验证所有的 TP 都是有效的，即它们必须把处于一个有效状态中的 CDI

转换到另一个有效状态。安全管理员必须为每一个 TP 及其所能操作的 CDI 集合定义对应关系，对应关系的格式是（TP_i，（CDI_a，CDI_b，CDI_c，…）），这个关系表列出了给定的 TP 可以操作的所有 CDI。

规则 E1 系统必须维护规则 C2 中描述的关系表，对于任意的 CDI，系统必须确定只有关系表中列出的对应 TP 才能对该 CDI 进行操作。

以下规则对 C-W 模型的基础框架进行拓展，以支持职责分离原则。

规则 E2 系统必须维护一个确定用户、TP 和 CDI 集合之间关系的关系表，关系的格式为（UserID，TP_i，（CDI_a，CDI_b，CDI_c，…）），其中，UserID 是用户标识。系统必须确保只有某个关系中指定的用户才能执行指定的 TP 对指定的 CDI 进行操作。

规则 C3 必须证明规则 E2 中的关系表满足职责分离要求。

以下规则实现用户身份认证，以支持规则 E2 中要用到的用户标识。

规则 E3 系统必须认证试图执行 TP 的每个用户的身份。

几乎所有实施完整性的系统都要求对所有 TP 的执行进行审计，提供审计记录。审计记录是特定形式的 CDI，以下规则提供审计支持。

规则 C4 必须证明所有的 TP 都向一个只能以附加方式写的 CDI 写入足够的信息，以便能够重现 TP 的操作过程。

系统中除了包含 CDI 以外，也包含 UDI，从系统外部进入到系统中的新信息就属于 UDI，如用户从键盘上输入的新信息。以下规则说明对 UDI 的处理方法。

规则 C5 必须证明接收 UDI 输入的 TP 对 UDI 的任何可能取值，要么只进行有效转换，要么不进行转换。即 TP 把输入的 UDI 转换为 CDI 或者拒绝相应的 UDI 输入。在典型情况下，这样的 TP 是编辑程序。

为了确保 C-W 模型的有效性，不能忽略任何一个证明规则。例如，用户不能创建并且运行一个没有经过证明的新的 TP，否则系统就达不到它的有效性目的。为此，系统需要以下规则加以约束。

规则 E4 只有有权对实体（如 TP）进行证明的主体才能修改这些实体与其他实体（如 CDI）之间的关系表。有权对某个实体（如 TP 或 CDI）进行证明的主体不能拥有与该实体相关的执行权。

修改实体的关系表就是修改实体的访问控制配置属性，假设某实体的属主有权修改实体的关系表，那么，根据规则 E4，该实体的属主不能拥有与该实体相关的执行权，但是，实际上，一个实体的属主是拥有与该实体相关的执行权的，这样便产生了矛盾，所以，假设不能成立，即一个实体的属主不能修改该实体的访问控制配置属性，因此，规则 E4 确定了 C-W 模型不是一个自主访问控制模型，它是一个强制访问控制模型。

（3）模型的概括。

Clark-Wilson 模型定义了 C1～C5 5 个证明规则和 E1～E4 4 个实施规则，这 9 个规则共同定义一个实施一致的完整性策略的系统。由这 9 个规则构成的 C-W 模型可以用图 3.2 进行概括。

C-W 模型从良构事务和职责分离两个方面构造完整性控制框架，它把系统中的数据项划分为约束数据项和非约束数据项两大类，通过转换过程和完整性验证过程定义系统的行为，依靠证明规则和实施规则实现对系统行为的约束，进而支持一致的完整性控制策略。

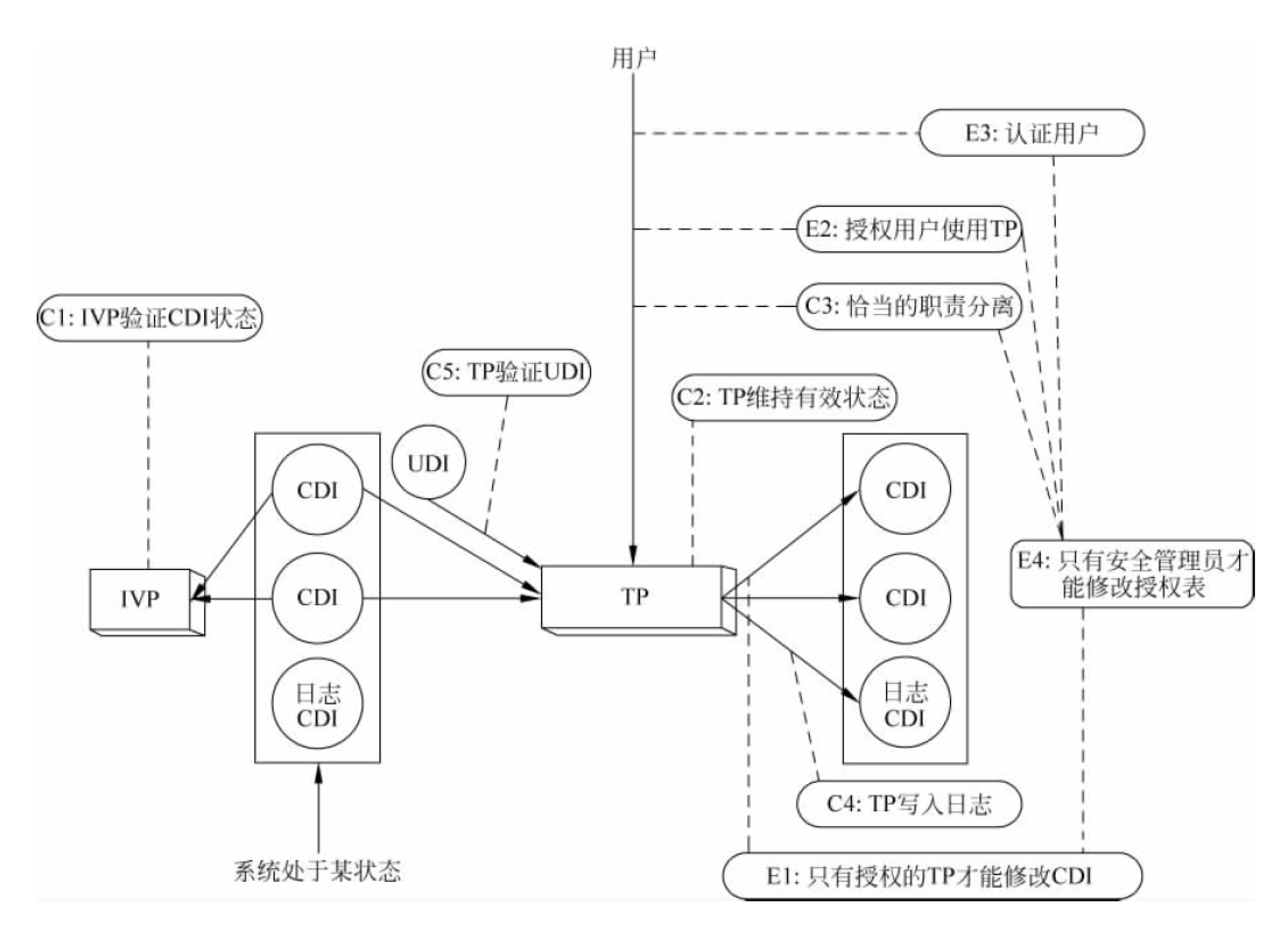


图 3.2　Clark-Wilson 模型的系统完整性规则

3.3.2　安全规划方法

在开展信息系统的安全建设之前，需要在安全专家的指导和帮助下，首先对信息系统的基本情况和安全风险进行科学全面的评估，从而更为准确、全面地了解信息系统的安全需求，以此为参考为客户进行总体规划和详细安全方案设计，提供最恰当的安全控制措施及安全管理策略来降低安全风险，最终帮助客户实现真正意义上的全网安全。

信息系统是一个复杂的巨系统，信息系统的安全建设是一个系统工程，因此从系统的安全风险评估、安全需求分析，到安全总体规划、详细安全设计，再到安全产品选择与安全集成以及安全管理策略的制定都要参照系统工程学的方法和思路。

信息系统安全规划依托企业信息化战略规划，对信息化战略的实施起到保驾护航的作用。信息系统安全规划的目标与企业信息化的目标是一致的，而且应该比企业信息化的目标更具体明确、更贴近安全需求。信息系统安全规划的一切论述都要围绕着这个目标展开和部署。

信息系统安全规划的方法和侧重点均可以有所区别，但是需要围绕技术安全、管理安全以及组织安全进行全面的考虑。规划的内容应该包括：确定信息系统安全的任务、目标、战略以及战略部门和战略人员，并在此基础上制定出物理安全、网络安全、系统安全、运营安全和人员安全的信息系统安全的总体规划。其中，物理安全包括环境设备安全、信息设备安全、网络设备安全以及信息资产设备的物理分布安全等；网络安全包括网络拓扑结构安全、网络的物理线路安全、网络访问安全（防火墙、入侵检测系统、VPN 等）等；系统安全包括操

作系统安全、应用软件安全以及应用策略安全等；运营安全应在控制层面和管理层面保障，包括备份与恢复系统安全、入侵检测功能、加密认证功能、漏洞检查及系统补丁功能、口令管理等；人员安全包括安全管理的组织机构、人员安全教育与意识机制、人员招聘及离职管理、第三方人员安全管理等。

信息系统安全规划的最终效果应该体现在对信息系统与信息资源的安全保护上，因此规划工作要围绕着信息系统与信息资源的开发、利用和保护工作进行，并且包括蓝图、现状、需求及措施4个方面。首先，对信息系统与信息资源的规划需要从信息化建设的蓝图入手，明确企业信息化发展策略的总体目标和各阶段的实施目标，制定出信息系统安全的发展目标；第二，对企业的信息化工作现状进行整体、综合、全面的分析，找出过去工作中的优势与不足；第三，根据信息化建设的目标提出未来几年的需求，这个需求最好可以分解成若干个小的方面，以便于今后的落实与实施；第四，明确实施工作阶段的具体措施与方法，提高规划工作的执行力度。

信息系统安全规划服务于企业信息化战略目标，信息系统安全规划做得好，企业信息化工作的实现就有了保障。信息系统安全规划是企业信息化发展战略的基础性工作，不是可有可无而是非常重要。由于企业信息化的任务与目标不同，所以信息系统安全规划包括的内容就不同，建设的规模也有很大的差异，因此信息系统安全规划无法从专业书籍或研究资料中找到非常有针对性的帮助和适用法则，也不可能给出一个规范化的信息系统安全规划的模板。信息系统安全规划的框架与方法的给出还需要依赖信息系统安全规划工作的建设原则、内容和思路，在具体规划中还需要深入细致地进行本地化的调查与研究。

3.4 本章小结

本章首先介绍了信息系统安全规划的概念、目标、作用和步骤，然后深入介绍信息系统安全规划的内容，包括计算模式的安全规划、信息资源的安全规划、网络与系统安全规划、组织与管理安全规划。计算模式规划方面主要介绍了近年来比较流行的C/S、B/S模式的安全规划方法，并粗略涉及近期比较流行的云计算模式。信息资源的规划强调保障信息的完整性、保密性和可用性。网络与系统的安全规划具体到网络拓扑结构、网络通信及系统面临的安全威胁等的安全防御措施。组织与管理安全规划是信息系统安全规划不可忽视的问题，所谓“三分技术，七分管理”就是这个道理。最后采用分类列举的方式详细介绍安全规划模型和方法，包括几种典型的安全模型，例如，比较经典的BLP模型、Biba模型和RBAC模型等。

3.5 习题

1. 信息系统安全规划的目的是什么？
2. 你认为信息系统安全规划的步骤中最重要的是哪一点？为什么？
3. 了解多种安全模型，举例说明信息流模型与访问控制模型的优缺点。

4. 你对信息系统的安全规划方法还有什么更多的认识?

5. 所谓规划是为了防止危险以及应对危险的发生,分析信息系统的安全规划与信息安全规划的关系。

6. 熟悉本章对 BLP 模型的描述,你认为 BLP 模型还有什么地方可以改进?

7. 仔细阅读本章所涉及的一系列的安全模型并查阅相关资料,对这些模型进行分析和比较。

8. 信息系统主要的安全规划方法有哪些?

第4章　信息系统安全需求

目前，很多企业单位虽然知道信息安全的严重性，但不知道怎么去防护，有的随意购买一些安全产品就以为万事大吉了，实际上这是远远不够的。出现这类情况的根本原因是这些企业单位对自己的总体的安全需求不清楚，安全需求是一个企业为保护其信息系统的安全对必须要做的工作的全面描述，是一个很详细、全面、系统的工作规划，是需要经过仔细的研究和分析才能得出的一份技术成果。为一个企业设计一个安全体系，对企业的安全需求进行分析是必不可少的，是对企业的信息财产进行保护的依据。安全需求分析工作是在安全风险分析与评估工作的基础上进行的，是安全工程学中的另一个阶段的工作。

4.1　安全需求概述

对安全需求的理解可以从多角度、多侧面入手，安全工程应该是全方位的，应从安全性、可靠性、高效性、可控性和持续性等多方面落实。

4.1.1　安全需求的来源

系统安全需求详细规定系统的安全功能和安全功能要达到的目标，并以此作为选择系统安全措施的标准。安全需求一般都衍生自以下3种来源。

1. 风险评估结果

(1) 风险评估人员根据组织的安全策略、安全目标和系统安全等级确定出适合系统的安全基线，以此作为安全要求的直接输入。

(2) 风险评估人员对系统进行基于关键资产的风险分析和排序，确定出需要降低的安全风险。

这是针对特定信息系统构成及业务特点进行风险评估得到的结果。

2. 国家信息安全法律法规对组织信息系统安全的要求

信息系统安全建设要遵守国家的法律、法规和相关的行业标准。比如财政部和各省的财经项目，其安全建设必须在制定安全需求时满足国家出台的《计算机安全保护条例》及财政系统提出的《政府财政管理信息系统安全总体标准》和《政府财政管理信息系统安全保障体系》等行业标准。

3. 组织业务性质确定的特殊要求

安全需求的第三种来源是组织业务性质确定的特殊要求。例如，IT系统支持的企业电子商务平台要保障其正常运行。对商务信息的机密性、完整性和可用性的要求就要体现在系统的安全需求中。安全需求还应包括对其贸易伙伴、合同方及服务提供者必须予以满足的那些合同所规定的和法定的要求。

4.1.2　不同层次的安全需求

在结合国家政策法规、企业性质和规章制度的基础上，考虑安全生产的各方面的要求，提出安全要求与安全级别；根据对象单位资产的确认情况，提出不同资产的安全级别需求，这样，安全问题就可以有的放矢。因为信息与网络系统是分层的，所以，在进行需求分析时也应该根据各层的具体情况分级别提出安全需求。一般情况下，要考虑以下 5 个层次的安全需求。

1. 物理层的安全需求

在考虑信息系统安全时，首先要考虑物理安全。例如：不规范施工、设备毁坏、意外故障、物理区访问控制等。物理层的安全就是保证实体财产的安全。实体安全是信息系统安全的低层安全，也是保证上层安全的基础。物理层的安全需求分析就是根据单位的实际情况，确定单位各实体财产的安全级别，需要什么程度的安全防护，达到什么样的安全目的。通常对于涉密信息，应防止系统通过无线电辐射泄露秘密信息等。

2. 系统层的安全需求

这里的系统主要指操作系统，操作系统是信息系统的基础平台，它的安全也是保证上层安全的基础。系统层的安全主要是保证主机，特别是各应用服务器和数据库服务器的操作系统、应用软件及其数据的安全。Internet 上的各种网络攻击主要集中在系统层，包括对各种操作系统、应用服务器、网络基本服务的攻击，利用这些操作系统、应用服务器、网络服务的安全漏洞，取得对服务器的控制权。这些攻击可能在信息网络内部，也可能在信息网络外部出现。此外，病毒也可能进入信息网络中传播，对各种主机和服务器造成破坏，导致系统不可用、文件损坏、数据丢失等严重后果。

系统层的安全需求分析就是研究为保证安全，应该要求操作平台达到什么样的安全级别，为达到所要求的级别，应该选用什么样的操作系统，如何使用、管理、配置操作系统。

3. 网络层的安全需求

网络层是 Internet 的核心，是为上层应用提供网络传输的基础，也是局域网和广域网连接的接口。因此，针对网络层的攻击和破坏很多。现在经常采取的安全防护措施是在网络的边界上，通过部署防火墙产品的 IP 过滤和应用代理等功能来实现安全连接，抵御来自公共网络的各种攻击，保障内部网络的正常运行。

网络层的安全需求还包括：

(1) 对内部网络不同安全区域有不同的安全需求，做不同的安全访问控制措施。

(2) 对于重要的服务器、网络交换、路由设备的系统日志，采取集中的基于行为的审计，从根本上防止别人利用信息网络的系统及设备进行攻击。

(3) 对于需要在公共网络中传送的重要数据，使用 VPN 技术实现机密传输，以保证重要信息的机密性和完整性。

(4) 建立网络安全主动防御机制，采用基于主机的入侵检测系统部署防范针对主机的攻击，采用基于网络的入侵检测系统对信息网络的重要网段提供主动性安全保证措施。

(5) 对于网络层所传输的数据的保护可以采用加密技术来实现，新一代的安全网络协议正在设计和实验阶段。那么，根据信息系统的业务方向，分析系统的网络安全需求，再确

定应该采用什么样的防护方式。

4. 应用层的安全需求

应用层是网络分层结构的最上层，是用户直接接触的部分。由于基于网络的应用很多，供应商也很多，所以存在的安全问题也很多，相应的安全防护技术也很多，需要根据实际情况来衡量对它们的需求程度。

5. 管理层的安全需求

信息系统安全是一个管理和技术结合的问题。一个严密、完整的管理体制，不但可以最大限度地在确保信息系统安全的前提下实现信息资源共享，而且可以弥补技术性安全隐患的部分弱点。管理包括行政性和技术性管理。信息系统能否正常高效地运行，很大程度上取决于是否发挥了它的最大功效，这依赖于系统的管理策略。管理层的安全需求分析就是研究为了保证系统的安全，应该建立一个怎样的管理体制。具体来讲，就是成立什么样的管理机构或部门，负责什么任务，完成什么功能，遵循什么原则，达到什么要求。

4.2 安全需求分析概述

安全需求分析是为了在安全系统的开发人员和提出需求的人员(即用户)之间建立一种理解和沟通的机制，以确定安全系统"做什么"而非"怎么做"，即如何实现的问题。安全需求以一种清晰、简洁、一致且无二义性的方式，对一个待开发的安全系统中各个有意义的方面进行陈述，它必须包含有足够多的信息，以使开发人员开发一个能使用户满意的安全系统。

4.2.1 安全需求分析涉及的一般性问题

本节主要是考察在安全目标、需求和要求的分析和定义中所涉及的一般性问题。

1. 安全法规和策略

首次信息系统安全的需求分析活动应包括全面审查和考虑适用规定和政策法令。此过程中需要解释大量的法规、法令、规定、机构的政策、政府有关保护机密信息的指南、国家标准等，其目的是保证系统充分实现强制性规定以及相关的指南得到遵守。ISSE 过程并不要求产生系统特有的策略或指令，而是把这些指令视为对任务环境和用户机构更合适的较高层次的管理功能。安全的接口控制和设计规范以及系统安全操作程序、限制和控制都应作为系统产品和过程方案在整个开发周期内的 ISSE 过程中产生出来。

2. 安全威胁评估

安全威胁评估定义为敌方有意利用对信息或系统造成损害的环境、行动或事件的能力、意图、攻击目标和方法。既要考虑内部和外部人员的故意安全威胁，也要考虑误操作或偶然的误用。ISSE 与用户一起工作，帮助他们在系统威胁评估报告(System Threat Assessment Report，STAR)中准确描述有关信息系统安全的威胁。

STAR 的内容包括：

(1) 开发期间的威胁。

(2) 信息和信息系统的安全威胁。

(3) 其他各种类型的威胁。

(4) 得到证明的威胁。

(5) 可以支持的假设威胁。

3. 任务安全目标

安全目标由系统用户陈述,代表最高等级的安全定义。安全目标可以适用于任务的某个部分,也可以适用于任务的多方面。一个具体的安全目标说明应对得到安全目标支持的任务进行文档化描述。作为系统能力需求定义的一部分,应对安全目标和基本理由陈述建立有效的可追踪性。

安全目标如图 4.1 所示,图中显示了任务信息、通用性威胁指南、综合安全指南和安全目标的关系。理由说明应提供对某些需要安全保护的理解,并抓住安全目标与以下各项之间的关系:受到安全目标支持的任务目标、激发安全目标与任务相关的威胁、不实现安全目标的后果、驱动或支持适用于安全目标的综合安全指南。

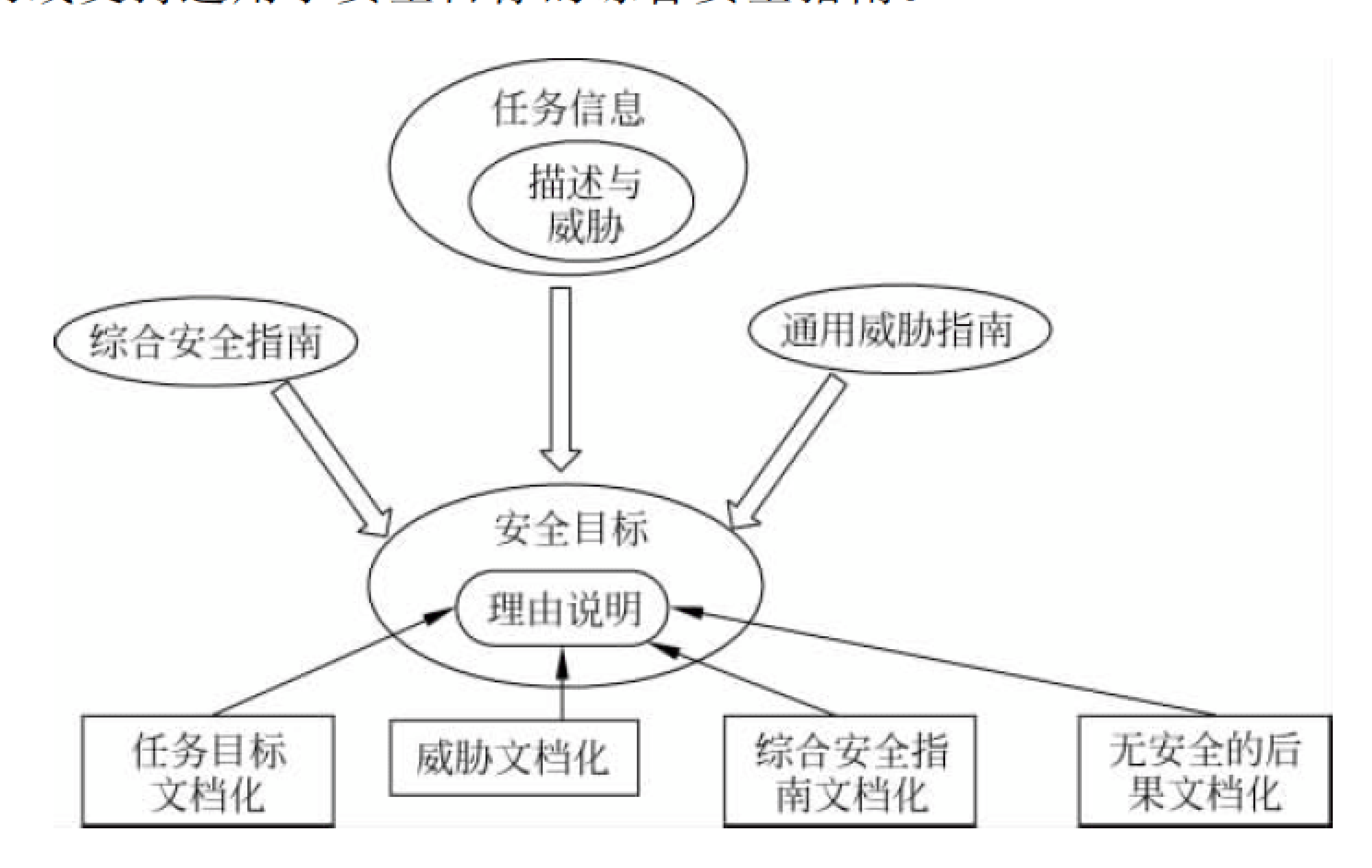


图 4.1　安全目标

4. 安全服务

在对威胁进行分析的基础上,规定了 5 种标准的安全服务。

1) 对象认证安全服务

对象认证安全服务用于识别对象的身份并证实。OSI 环境可提供信源认证和对等实体认证等安全服务。信源认证是用于验证收到的数据来源与所声称的来源是否一致,它不提供防止数据中途被修改的功能。对等实体认证是用来验证在某一关联的实体中,对等实体的声明是一致的,它可以确认对等实体没有假冒身份。

2) 访问控制安全服务

访问控制安全服务提供对未授权使用资源的防御措施。访问控制可分为自主访问控制、强制访问控制、基于角色的访问控制。可以通过基于访问控制属性的访问控制表、基于安全标签或用户和资源分档的多级访问控制等实现。

3) 数据机密性安全服务

数据机密性安全服务是针对信息泄露而采取的防御措施,可分为信息保密、选择段保密

和业务流保密。它的基础是数据加密机制的选择。

4）数据完整性安全服务

数据完整性安全服务是防止非法篡改信息，如修改、复制和删除等。它有5种形式：无连接完整性、选择字段无连接完整性、可恢复连接完整性、无恢复连接完整性、选择字段连接完整性。

5）防抵赖性安全服务

防抵赖性安全服务是针对对方抵赖的防范措施，用来证实发生过的操作，它可分为对发送防抵赖和对接收防抵赖。

另外，还可以包括鉴别服务和可用性服务。

鉴别服务是对用户、用户设备和其他实体进行有效性验证和真实性验证，或对被存储或被传输的完整性提供保护，即防止其他实体占用或独立操作被鉴别实体的身份。

可用性服务是保证提供按用户所需的地点、时间和形式的信息。

4.2.2 安全需求分析过程

信息系统安全需求的分析过程一般来说主要有以下基本的步骤。

1. 系统调查

了解信息系统所处的安全环境，即存在于系统边界之外并对系统的安全具有直接或潜在影响的所有因素及其他与安全相关的信息，如用户、组成部件、运行机制及与其他系统的连接情况等。在此基础上确定需要保护的资产，包括软硬件、数据、文档和计算机服务等，并评价各个资产的相对价值。

2. 定性分析系统的脆弱点和可能遭受的安全威胁

此步骤需要一定程度的想象，以预测资产可能受到的损害及损害的来源，因此比第一步更加困难。系统脆弱点和安全威胁是两个互相依赖的概念。没有脆弱点，威胁也就不成“威胁”；没有威胁，也就没有所谓的脆弱点。当系统的脆弱点被确定后，需要针对各脆弱点分析可能由此引发的安全威胁及其对资产可能造成损害程度。

3. 定量分析脆弱点和安全威胁

此步的目标是确定系统暴露各种脆弱点及面临安全威胁的可能性。这种可能性与当前所处的安全环境和采用的安全措施有关。估算脆弱点和安全威胁的可能性是非常困难的，一般主要采用概率统计的方法。分析的数据主要是操作日志，局部犯罪的统计和用户的投诉等，得到结果后可以进一步计算出系统承受的安全风险值。

4. 需求的确定

此步将定性分析和定量分析的结果进行综合，定义信息系统的安全需求。开发人员由此确定相应的安全措施，为信息系统提供有效且合理的安全保障。

安全需求分析的过程是一个不断发展的过程。随着系统环境的发展以及外部形势的改变，安全需求也会改变。要想保持分析结果的有效性，必须保证结果时刻最新，安全需求分析的过程也得与系统同步发展。安全需求的管理工作也将一直进行下去，以最终指导信息系统安全保障措施的实施。

4.2.3 安全需求分析方法

1. 安全危险性分析模型

安全需求的获取实际上是对用户意图不断进行揭示和判断的过程。当用户在对信息系统自身的状况和可能遇到的安全危险并不太了解的情况下，只能提出一些较为抽象的安全需求。安全危险性分析的目的就是对各种危险信息进行全面的收集和充分的分析，以使用户能够进一步明确系统的脆弱点和可能遭受的安全威胁，从而提出详细、准确的安全需求。

2. 安全风险分析模型

安全风险是由于某种不希望安全事件的发生，导致对系统造成影响的可能性。根据系统安全工程能力成熟模型(SSE-EMM)中的理论，能够成为风险的安全事件有 3 个重要的组成部分：系统脆弱点、安全威胁和事件造成的影响。一般而言，这 3 个因素必须同时存在才能构成安全风险。

信息系统面临的安全风险值是确定系统安全需求的一个重要依据，也是评价系统安全可信度的一个重要的量化指标。确定了可能受到损害的资产，并分析出相应的脆弱点和安全威胁后，就可以通过安全风险分析确定系统资产的风险所在，再采用相应的安全措施将信息系统遗留的安全风险控制在可接受的范围之内。图 4.2 给出了安全风险分析的全过程。

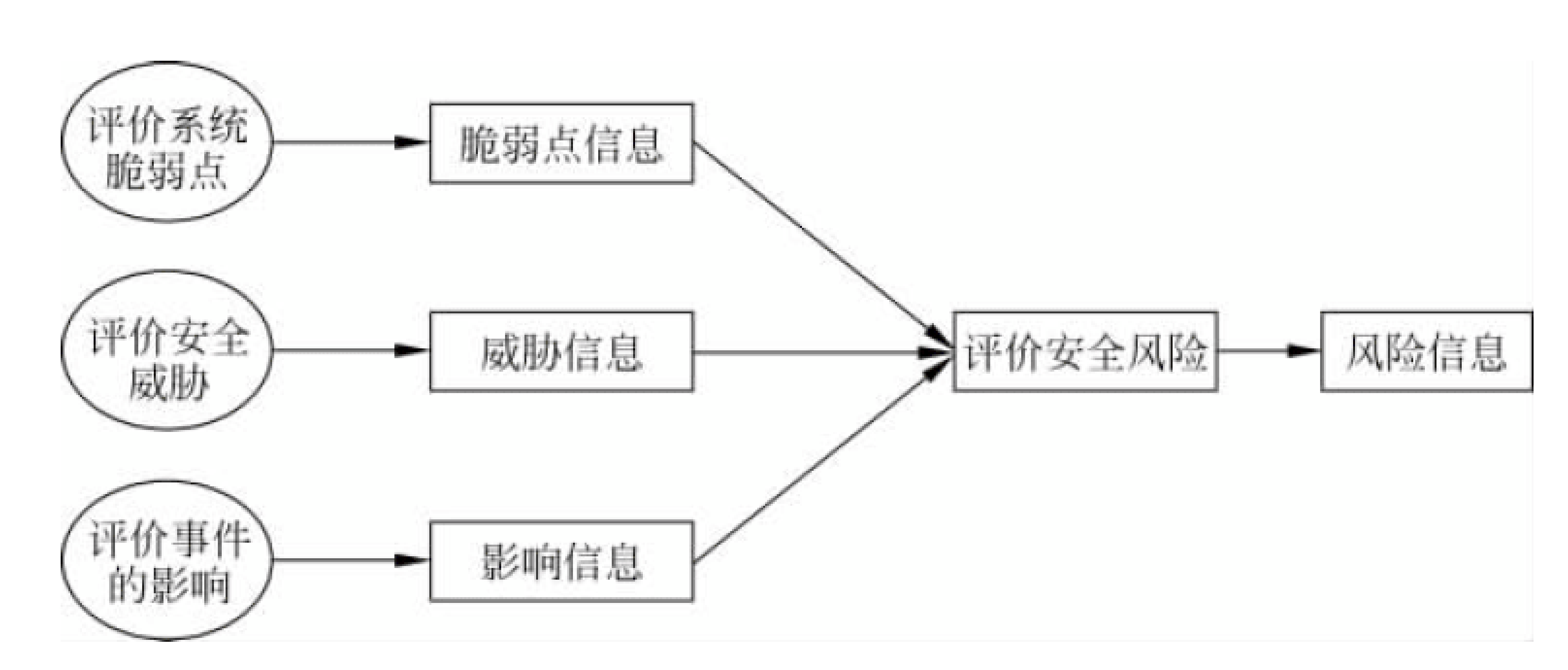


图 4.2 安全风险分析过程

4.2.4 安全需求的描述方法

很多人用自然语言来描述安全需求。自然语言的好处是直观、易懂、交流方便，但隐藏了可能导致误解的模糊成分。特别是对于需要精确、简洁描述的安全需求来说，自然语言的二义性可能导致开发人员对用户需求的误解，隐藏的模糊成分可能导致安全系统某些功能自相矛盾。

软件工程中使用形式化、非形式化和基于知识表示的需求规格说明方法描述安全需求，它们各有优缺点，但由于其缺乏对安全领域知识的描述能力，因此在描述安全需求方面存在着某些不足。例如形式化方法虽然能够严密、精确地描述和分析安全需求，但是其非常复杂而且难以掌握，不易于被非专家级的人员理解，从而不便于和用户沟通。应用仍存在一定的局限性。

被国际标准化组织认可的通用标准中给出了一套安全需求的定义方法，供安全系统的

开发人员、用户和评价人员参照使用。通用标准中，安全需求以类、族和组件的形式进行定义，其中类和族反映的是分类方法，具体的安全需求由组件来体现。通常，安全系统有多项安全需求，需要用多个需求组件以一定的组织方式组合起来表示。通用标准定义了3种类型的组织结构用于描述系统的安全需求：安全组件包、保护框架定义书(Protection Profile，PP)和安全对象定义书(Security Target，ST)。

采用通用标准中的描述方法，可以产生标准化的需求规格说明，而且便于对安全系统进行有效的安全评估。缺点是由于描述语言的形式化程度不高，不便于对安全需求进行一致性和完备性的验证，并且缺乏对定量化的安全保障需求的描述。解决的方法是结合使用其他的描述方法，将通用标准的需求规格说明方法进行扩展。

4.3 安全需求分类

用户对安全方面的需求有很多，涉及待开发系统的功能、性能和约束等各个方面的内容。信息技术安全性认证通用标准将安全需求划分成安全功能需求和安全保障需求两个独立的范畴来定义，前者描述的是安全系统应该提供的安全功能，后者描述的是系统的安全可信度及为获取可信度而应该采取的措施。

4.3.1 操作系统安全需求

操作系统作为管理和调度中心，保证用户能够高效、有序地使用计算机资源。操作系统服务多个应用软件和用户，确保多个应用软件和用户能够安全地使用系统资源是最基本的安全目标之一。下面初步分析操作系统的安全需求。

对于多用户操作系统，在用户管理上存在一系列的安全问题。例如，对于一台公用计算机，多个用户使用时必须要考虑用户管理问题。如果任意用户都拥有资源的控制权限，任何人都可以更改系统配置、设置文件访问权限等，那么其他用户的程序或文件可能无法使用了，保存的信息也没有了机密性，用户彼此之间冲突导致系统崩溃。因此，操作系统要管理用户账户及权限，提高用户信息与应用程序的安全性。

另外，进程之间对资源的竞争也可能导致操作系统不安全。在系统中并行运行着多个进程，进程之间共享CPU，存在CPU和内存空间的竞争。若一个进程越界访问并更改了其他进程的内存空间，将导致其他程序无法执行。进程对资源的占用是互斥的，当某个进程长期占用某一资源时，如果没有进程管理和保护策略，其他需要使用此资源的进程将无法运行，导致操作系统面临死锁的问题。

操作系统本身就是一个基本的信息系统，有着与普通信息系统类似的安全需求。例如为用户文件信息提供保密服务，对异常系统行为有责任认定的能力。由于操作系统自身的重要性和复杂性，客观上需要有严格验证其安全性的方法。

4.3.2 数据库安全需求

数据库安全包括两方面的问题：一是数据库数据的安全，二是数据库系统不被非法用户入侵。数据库数据的安全指当数据库数据存储媒介被破坏时以及当数据库用户误操作

时，数据库数据信息不至于丢失。数据库系统不被非法用户入侵是指尽可能地发现各种潜在的漏洞，防止非授权用户利用漏洞入侵数据库系统。数据库的安全需求可以总结为以下方面：

1. 数据机密性

数据机密性是指数据不会受到未授权用户的访问，即敏感信息不会直接或间接地泄露给未授权用户。数据库管理系统（DBMS）在决定是否运行一个访问时，需要考虑数据的可用性、访问的可接受性及用户的合法性。

2. 数据完整性

数据完整性主要指数据库中的数据必须满足相关约束，以满足所支撑业务处理的要求。当整个数据库或某个数据项被破坏时，数据的完整性受到破坏。数据库完整性包括物理数据库完整性和逻辑数据库完整性。

物理数据库完整性是指整个数据库的数据不受物理条件的影响，在灾难发生后可以重建数据库。

逻辑数据库完整性是指数据库的结构是受到保护的。

3. 可用性

可用性是指当系统授权的合法用户申请访问授权数据时，安全系统应保证该访问的可操作性。

4. 可靠性

可靠性包括操作可靠性和存储可靠性。

操作可靠性主要指数据库往往是重要业务操作的对象，操作一般分为多个步骤，为了不破坏数据，需要确保操作作为一个整体成功或失败。

存储可靠性是指数据库需要提供可靠的方法存储数据，减小系统故障、数据丢失或损坏的风险。

5. 可追踪性

可追踪性是指能够跟踪到访问或修改数据元素的人，以帮助维护数据库的完整性。

4.3.3 网络安全需求

满足基本的安全要求，是网络成功运行的必要条件，在此基础上提供强有力的安全保障，是网络系统安全的重要原则。网络内部部署了众多的网络设备、服务器，保护这些设备的正常运行，维护主要业务系统的安全，是网络的基本安全需求。对于各种各样的网络攻击，在提供灵活且高效的网络通信及信息服务的同时，抵御和发现网络攻击，并且提供跟踪攻击的手段。网络基本安全需求主要表现为：

(1) 网络正常运行。在受到攻击的情况下，能够保证网络系统继续运行。

(2) 网络管理和网络部署的资料不被窃取。

(3) 具备先进的入侵检测及跟踪体系。

(4) 提供灵活而高效的内外通信服务。

与普通网络应用不同的是，应用系统是网络功能的核心。对于应用系统应该具有最高

的网络安全措施。应用系统的安全体系应包含：

(1) 访问控制。

通过对特定网段、服务建立的访问控制体系，将绝大多数攻击阻止在到达攻击目标之前。

(2) 检查安全漏洞。

通过对安全漏洞的周期检查，即使攻击可到达攻击目标，也可使绝大多数攻击无效。

(3) 攻击监控。

通过对特定网段、服务建立的攻击监控体系，可实时检测出绝大多数攻击，并采取相应的行动，如断开网络连接、记录攻击过程、跟踪攻击源等。

(4) 加密通信。

主动的加密通信，可使攻击者不能了解、修改敏感信息。

(5) 认证。

良好的认证体系可防止攻击者假冒合法用户。

(6) 备份和恢复。

良好的备份和恢复机制，可在攻击造成损失时，尽快地恢复数据和系统服务。

(7) 多层防御。

攻击者在突破第一道防线后，延缓或阻断其到达攻击目标。

(8) 隐藏内部信息。

使攻击者不能了解系统内的基本情况。

(9) 设立安全监控中心。

为信息系统提供安全体系管理、监控、维护及紧急情况服务。

4.3.4　物联网安全需求

物联网被公认为包含 3 个层次，从下到上依次是感知层、网络层和应用层。

物联网的末端节点包括：传感器节点、RFID 标签、近距离无线通信终端、移动通信终端、摄像头以及传感网络网关等。按照末端节点与网络的关系划分，有接入感知网络的节点以及直接接入通信网络的节点。物联网的安全需求可分为以下 4 个方面。

1. 末端节点的安全需求

末端节点的安全需求可通过对节点特性的分析归纳得出，这些特性包括：

(1)节点的存储、通信及处理能力等物理特性。

(2)节点所提供服务的差异。

(3)节点所服务的环境及使用用户要求的差异等。

不同特性节点的脆弱性与安全威胁、安全防护要求及可能采取的安全措施也各不相同。

2. 感知层安全需求

感知网络的安全需求应该根据感知网络自身的特点、服务的节点特征及使用用户的要求进行建立。一般的感知网络特点包括：低功耗、分布松散、信令简练、协议简单、广播特性、少量交互甚至无交互等，因此安全建立应利用尽可能少的能量及带宽资源，设计出精简、安全的算法、密钥体系及安全协议，解决相应的安全问题。

3. 网络层安全需求

通信网络主要包括有线、无线及卫星信道等，通信网络的安全问题早在通信网络标准制定初期，就被国际及国内相关标准组织、研究院所及管理机构所研究，并制定了一系列标准算法、安全协议及解决方案。通信网络的安全需求主要包括：

(1) 接入鉴权。

(2) 话音、数据及多媒体业务信息的传输保护。

(3) 在公共网络设施上构建 VPN 的应用需求，用户个人信息或集团信息的隐蔽。

(4) 各种网络病毒、网络攻击等。

针对不同的网络特征及用户需求，采取一般的安全防护措施或增强的安全防护措施能基本解决物联网通信网络的大部分安全问题。

4. 应用层安全需求

安全问题及安全需求研究需结合各个应用层次分别开展研究，各层次的安全问题及安全需求存在共性及差异。共性的安全需求包括：操作用户的身份认证、访问控制，对敏感信息的信源加密及完整性保护、证书及身份鉴别、数字签名及抗抵赖、安全审计等。个性化的安全需求需要针对各类应用的特点、使用环境、服务对象及用户特殊要求等进行分析研究。

4.3.5　云安全需求

从客户的角度看，使用“云”的客户对“云”自身的安全要求，与传统网络及系统是类似的。客户看重的仍然是放在“云”上的基础数据是否安全。在云计算环境下，由于网络层和系统层的抽象化，客户在使用云计算提供商提供的云环境时，为保证数据的机密性、完整性、可用性、真实性、授权、认证和不可抵赖性，会特别关注以下几个方面的安全需求。

1. 数据的机密性与完整性

在云计算下，客户端演变成显示终端，客户的私有数据存储在“云”上，数据传输、交换都发生在云计算提供商的“云”里。因此，保证放在“云 ”中属于客户的数据的机密性和完整性成为关键问题。云计算提供商应能有效维护数据的机密性和完整性，周期检测其运行状况并提交报告给客户。

2. 数据的存储位置

保证所有的数据包括所有副本和备份存储在规定的地理位置。具有相对固定的存储位置，使随时查看数据是否完整、可用和真实变得可行，同时也意味着客户私有数据是相对稳定的。

3. 数据删除持久性

云计算中，提供商为了保证资源的利用率，会将客户的私有数据共存在同一物理存储实体。当某一客户的部分或全部数据提出删除需求，该数据占用的存储空间就会被释放并分配给其他客户使用。如果存在数据删除不彻底、可被恢复的可能，就会造成客户数据泄露等严重后果。数据必须彻底有效地去除才能被视为销毁。云计算的提供商必须提供一种可用的技术，保证云计算数据能被有效定位和销毁，并保证数据已被完全消除或无法恢复。

4. 保证不同客户数据混合时数据间的有效隔离

数据尤其是敏感数据，在使用、存储或传输过程中，如果没有任何补偿控制，不能与其他

客户的数据混合。云提供者应能根据服务和数据的类型使用不同的隔离技术，实现客户间以及客户不同类型数据间的彼此隔离。云中存储的机密数据必须通过访问控制和加密措施等进行保护。

5. 数据备份和恢复重建

必须保证云数据备份和云恢复计划的有效性，以防止数据丢失、意外的数据覆盖和破坏。运营商应能演示并证明其云计算具有全面有效的风险管理流程。

6. 数据发现

云计算提供商应保证在有需求时能发现特定的数据并确保法律和监管当局要求的所有数据可被找回。

4.4 信息系统各基本阶段的安全需求

4.4.1 信息系统规划阶段的安全需求

信息系统规划阶段的安全目标是明确信息系统安全建设的目的，对信息系统安全建设实现的可能性进行分析论证，设计出总体安全规划方案。信息系统规划阶段涉及的主要安全需求包括：明确安全总体方针；确保安全总体方针源自业务期望；描述所涉及系统的安全现状；提交明确的安全需求文档；明确风险评估准则并达成一致；描述从系统的哪些层次进行安全实现；对系统规划中安全实现的可能性进行充分分析、论证。

4.4.2 信息系统设计阶段的安全需求

信息系统设计阶段的安全目标是依据规划阶段输出的总体安全规划方案，设计信息系统安全的实现结构和实施方案。实现结构包括功能划分、接口协议和性能指标等；实施方案包括实现技术、设备选型和系统集成等。信息系统设计阶段的主要安全需求包括：设计方案符合系统建设规划；设计方案中的安全需求符合规划阶段的安全目标；评估用以实现安全系统的各类技术的有效性；对用于实施方案的产品需满足安全保护等级的要求；对自开发的软件要在设计阶段充分考虑安全风险。

4.4.3 信息系统实施阶段的安全需求

信息系统实施阶段的安全目标是按照规划和设计阶段所定义的信息系统安全实施方案，采购设备和软件，开发定制功能，集成、部署、配置和测试信息系统的安全机制，培训人员，并对是否允许系统投入运行进行批准监督。信息系统实施阶段的主要安全需求包括：确保采购的设备、软件和其他系统组件满足已定义的安全要求；确保定制开发的软件和系统满足已定义的安全要求；确保整个系统已按照设计要求进行了部署和配置，并通过整体的安全测试来验证系统的安全功能和安全特性符合设计要求；通过对相关人员的操作培训和安全培训，确保人员已具备维持系统安全功能和安全特性的能力；通过对系统投入运行前的批准监督，确保信息系统的使用已得到授权。

4.4.4　信息系统运行维护阶段的安全需求

信息系统运行维护阶段的安全目标是在信息系统经过授权投入运行之后，确保在运行过程中，以及信息或其运行环境发生变化时维持系统的正常运行和安全性。信息系统运行维护阶段的安全需求包括：在信息系统未发生更改的情况下，维持系统的正常运行，进行日常的安全操作和安全管理；在信息系统及其运行环境发生变化的情况下，进行风险评估并针对风险制定处理措施；定期进行风险再评估工作，维持系统的持续安全；定期进行信息系统的重新审批工作，确保系统授权的时间有效性。

4.4.5　信息系统废弃阶段的安全需求

信息系统废弃阶段的安全目标是确保对信息系统的过时或无用部分进行安全报废处理，防止信息系统的安全要求和安全功能遭到破坏。信息系统废弃阶段的安全需求是信息、硬件和软件的安全处置，防止将敏感信息泄露给外部人员。

4.5　本章小结

本章对安全需求的内容进行了概述，描述了安全需求的来源和分层结构的安全需求。简要介绍了安全需求分析的一般性问题，并详细介绍了安全需求分析的过程、方法等内容。介绍了几种常见信息系统的安全需求。最后介绍了信息系统的基本阶段的安全需求。

4.6　习　　题

1. 简述 5 个层次的安全需求。
2. 概述安全需求分析的一般性问题。
3. 概述安全需求分析过程。
4. 简述几种常见的信息系统的安全需求内容。
5. 简述信息系统各个基本阶段的安全需求。

第5章　信息系统安全设计

为了细化信息系统的安全体系结构并将其转化为稳定可生产、经济效益好的系统设计，需要进行全面详细的安全设计。安全体系结构将信息安全因素加入到系统的体系结构中，从整体上解决信息系统的安全问题。它描述了信息系统的安全机制、安全服务、安全特性以及满足安全需求的各基本要素之间的关系。信息系统安全体系结构的安全视图主要集中在信息系统的高级安全机制及安全服务上，安全功能应分配在接口、系统配置项及低级组件上，并解决安全组件、安全服务与安全机制之间的矛盾冲突，保持其相互依赖关系。

从安全系统、功能及技术等安全视图的角度分析，信息系统应包括3种安全体系结构视图，即安全系统体系结构、安全功能体系结构及安全技术体系结构。因此，信息系统安全设计应该包括对安全系统、安全功能及安全技术3方面的安全设计。从系统工程的角度分析，信息系统安全的生命周期包括任务阶段、概念阶段、需求分析阶段、系统设计阶段、配置审计阶段以及运行与维护阶段。因此信息系统安全设计应涵盖对生命周期各阶段的安全分析与设计。

5.1　信息系统安全体系结构设计

5.1.1　安全系统设计

安全系统是由与安全问题有关的若干因素通过相互联系、作用及制约而成的具有特定功能的有机整体。

系统设计的总体原则是保证设计目标的实现，并在此基础上使技术资源的运用达到最佳效果。在进行系统设计过程中，应遵循以下原则：

(1) 可靠性。可靠性是指信息系统抵御外界干扰的能力及受外界干扰时的恢复能力。可靠性是系统设计的一个重要指标及基本出发点，只有设计出安全可靠的系统，才能在实际应用中发挥应有的作用。一个成功的信息系统必须具有较高的可靠性，如信息保密性、抗病毒能力、灾难恢复能力、检错纠错能力等。

(2) 灵活性。为了延长系统的寿命，提高系统适应外界环境变化的能力，系统应具有较好的开放性和结构的可变性。采用模块化结构设计可以提高各模块间的独立性，尽可能减少各子系统间的数据依赖程度，同时便于模块的修改及更新。

(3) 系统性。在系统设计中，为了提高系统的设计质量，要从整体的角度进行考虑，实现系统的信息代码及数据组织结构的统一化及设计规范的标准化。

(4) 经济性。在满足信息系统安全需求的前提下，尽可能地降低系统的开销。例如，在硬件配置上并不是越先进越好，而应以满足应用需要为前提。系统设计要尽量简洁，避免不必要的复杂化，以便缩短处理流程与时间，减少处理费用。

(5) 简单性。在实现设计目标及安全功能的前提下，系统应该尽量简单。在设计过程

中，简单性体现在简化操作、系统结构合理清晰，易于维护和使用。

系统模型包括逻辑模型和物理模型。在系统分析阶段提出的模型称为逻辑模型，主要解决系统“做什么”的问题。而在系统设计阶段所提出的是物理模型，主要确定“怎么做”的问题。如果说系统分析阶段所提出的系统逻辑模型只是一种构想，那么系统设计阶段的任务就是将这种构想付诸实践，即在系统分析的基础上，将分析所得的逻辑模型设计成科学合理的物理模型。系统设计的主要任务包括：总体设计、代码设计、设计规范的制定、系统物理配置方案设计、数据存储设计以及计算机处理过程设计。

确定信息系统必须实现的安全功能需求以及如何实现该功能是系统开发的两个必要组成部分。据此，可以将安全生命周期划分为两大部分。任务阶段、概念阶段和需求阶段用于确定系统的安全功能的需求问题，而系统设计、配置审计和运行维护阶段则解决系统安全功能的实现问题。

系统设计是一个反复、周期性的过程。一方面，设计的过程是迭代或周期性的，存在于系统的整个生命周期中诸多阶段。需要注意的是，迭代并不是重复，每次迭代过程中都是针对不同的需求并修改以前的功能。另一方面，设计的过程可变并且可调整，系统设计的过程及步骤会随着设计者对功能需求理解的深入而增加或减少，使过程设计更合理全面并有效。为了使设计过程更加精细，可以采用自动工具对概要设计进行分析与提炼，从而形成详细设计。其中有些工具可以对系统设计进行模型化分析与测试。

系统设计活动将集中对系统功能体系结构和物理体系结构进行研究和阐明。

系统功能体系结构：为了系统地展现系统功能，将其整合成一个体系，从而形成系统功能体系结构，包括功能接口、物理接口、功能需求、性能需求以及设计的层次安排等。

系统物理体系结构：一种包括系统功能设计需求、物理接口及基础性物理限制等的系统过程解决方案。系统物理体系结构的过程包括：首先将物理设计形成文档，完成风险分析、有效性分析和技术过渡性计划，从而确定该体系结构在物理实现上的可行性；其次，识别各方面的安全需求，并编制配置文档和其他测试文件；最后，详细地定义系统解决方案。

功能的划分可通过面向对象设计、结构化系统设计或其他设计方法来实现。

5.1.2　安全功能设计

安全功能设计描述了信息系统发挥正常功能所应具有的安全防护能力，包括对信息安全、运行安全和物理安全的设计。其中信息安全设计措施包括身份认证、访问控制、信息加密等；运行安全设计措施包括入侵检测、病毒防御、应急响应、灾难恢复、安全审计、风险评估等；物理安全设计措施包括设备安全、环境安全及介质安全等。

1. 信息安全设计

信息安全的含义非常广泛，不仅包含对信息系统的软硬件及数据的保护，同时也保障系统及信息服务连续可靠正常地运行。信息安全主要保证信息的机密性、真实性、完整性、可用性、不可抵赖性和可控性。其根本目的是使内部信息不受外部威胁，因此信息通常需要加密，同时要求有身份认证和访问控制机制。

1）身份认证

身份认证是为信息系统提供用户身份信息以便进行相应授权访问的技术，身份认证技

术主要有：I&A 认证、基于 PKI/CA 的数字证书认证服务技术、生物身份识别技术等。I&A 是使用用户名、密码登录进行身份认证的技术，I&A 对于登录系统存在隐患很多，容易造成密码盗用。PKI/CA 技术能够实现双向认证，能够保障系统的抗抵赖性、完整性以及加解密等功能，基于 PKI/CA 的数字证书认证技术已经被广泛应用于身份认证领域。生物身份识别技术是附着在其他应用技术上的新型技术，它必须配备相应的识别设备，用身体特征或行为特征来识别用户，一旦登录，设备就识别用户的相应特征，并将这些特征和已知的以数字方式存储的特征进行比较。生物身份识别技术与 PKI 结合使用是实现身份认证较好的解决方案。

2）访问控制

访问控制是信息系统安全的核心策略之一，它与身份认证、信息加密等有机结合，构成了信息系统中传输、存储和处理数据的安全基础设施。访问控制在身份认证的基础上，根据用户身份及预定义的访问控制策略对用户提出的资源访问请求加以控制。通常系统管理员控制用户对服务器、目录、文件等资源的访问。访问控制的主要目的是限制访问主体对客体的访问，从而保障数据资源在合法范围内得到有效的管理与控制。

常见的访问控制类型有自主访问控制、强制访问控制和基于角色的访问控制。访问控制技术可以应用到信息系统安全的各个层面，包括网络层、操作系统层、数据库管理系统层以及应用系统层。在信息系统安全问题越来越突出的今天，访问控制技术是一种非常有效的安全手段，通过制定严格、合理并符合最小特权、多人负责和职责分离三原则的访问控制策略，可以有效防止非法用户入侵系统，尤其是防止内部和外部人员的越权访问，在很大程度上提升信息系统的安全性。

3）数据加密

数据加密是防止信息泄露，保护信息安全的重要屏障，也是保障数据机密性、真实性的重要措施。一旦非法用户对系统实施攻击并成功进入系统，将有可能获取任何信息。所以，对系统中的数据进行加密，尤其是对关键数据加密，显得尤为重要。因为采用高强度加密技术处理后，即使非法用户得到这些数据也无法轻易进行还原。常用的加密技术分为常规加密技术与密钥加密技术，密钥加密技术又分为对称密钥加密技术与非对称密钥加密技术。在实际应用中人们通常将常规密码和公钥密码结合在一起使用。

2. 运行安全设计

运行安全是指信息系统在运行过程中的安全必须得到保证，使之能对信息和数据进行正确的处理，正常发挥系统的各项功能。运行安全的主要措施包括风险分析、审计跟踪、备份与恢复、应急 4 个方面。

1）风险分析

信息系统的安全风险来自于资产、威胁及脆弱性。资产是一个完整信息系统的组成部分，是风险评估的对象，信息系统的资产包括物理资产、软件资产、数据资产及其他资产。人为或突发性的安全事件对资产破坏的后果称为影响，可以表述为资产的相对价值。威胁是指可能对资产或组织造成损害事故的潜在因素，威胁是客观存在的，不可能被消灭或改变。更确切地说，某一特定资产必然面临某些特定的威胁。脆弱性是指资产中能被威胁利用的弱点，弱点可能位于包括物理环境、业务流程、组织机构、软硬件、人员等各个方面。资产的脆弱性是资产所特有的，只能通过相应的安全措施降低其脆弱程度，而不能够完全被消除。

风险是威胁事件发生的可能性与后果的结合，威胁、影响和脆弱性构成风险的主要因素，它们紧紧围绕资产这个中心。风险分析是对信息和资产的威胁、影响和脆弱性及三者发生可能性的计算和分析。

2）审计跟踪

信息系统审计跟踪是一个通过收集和评价审计证据，判断信息系统是否能够维护数据的完整性、保护资产的安全性及可用性，被审计单位的目标是否得以有效地实现的过程。信息系统审计跟踪关注的重点是系统功能与系统需求是否基本一致、信息处理的关键过程是否合理、初步评价信息系统的运用效果。

3）备份与恢复

信息系统在遭受自然或人为灾害后，重新启动系统的软硬件设备及数据恢复正常运行的能力，即系统的灾难恢复能力。灾难备份与恢复是信息系统业务连续性规划的重要部分，涉及灾难风险评估与防范，特别是关键性业务数据、应用、流程的记录、备份和保护。

对于信息系统中的网络设备、网络线路、加密设备、计算机设备、应用系统、数据库、维护人员，都要采取备份措施，确保在需要时有备用资源可供调配和恢复。信息系统备份手段根据不同信息的重要程度及恢复时间要求分为实时热备份和冷备份。同一平台的系统应尽量使用同样的备份手段，便于管理和使用。信息系统的备份与恢复管理需要指定一个部门专门负责，并制定数据备份计划，对数据备份的时间、内容、级别、人员、保管期限、异地存取和销毁手续等进行明确规定。

4）应急响应

应急响应计划是在意外事件发生时，快速而准确地确认事件性质，采取积极应对措施来控制事件影响的进一步扩大、阻断事件进程，必要时，进行安全反击、追踪攻击点，占领主动地位。

当入侵攻击发生时，一个简单的应急响应过程包括以下几步：

（1）一旦检测到入侵攻击，立即启用应急响应策略。

（2）识别事件类型和攻击特征。

（3）迅速启动其他更加严格的防御措施（如防火墙规则）。

（4）关闭非关键运行系统。

（5）针对攻击来源升级或修补系统漏洞。

（6）启用紧急情况下的接管系统。

（7）若时间和技术条件允许，立即分析入侵信息并追踪入侵来源。

3. 物理安全设计

物理安全主要是通过实施物理隔离实现网络系统安全，是整个信息系统安全的前提，其目的是保护信息系统所处环境、相关的硬件设备、存储介质以及通信线路等免受自然灾害、人为破坏和搭线窃听攻击。

物理安全措施主要包括安全制度、数据备份、辐射防护、屏幕口令防护、隐藏销毁、状态检测、报警确认、应急恢复、加强机房管理、安全组织和人事管理等手段。

物理安全主要考虑的问题是环境、场地、设备的安全及物理访问控制和应急处理计划等，在整个信息系统中占据重要地位。它主要包括以下几个方面的内容。

1）机房环境安全

机房环境安全涉及机房安全技术及标准，机房安全技术涵盖范围极为广泛，机房从内至

外，从设备设施到管理制度都属于机房安全技术研究的范畴。包括计算机机房的安全保卫技术，温度、湿度和洁净度等环境条件保持技术，机房用电安全技术和安全管理技术。计算机场地建设应遵循国家标准《计算机场地通用规范》和《计算站场地安全要求》，满足防火、防磁、防水、防电击、防虫害等要求，并配备相应的设备。

2）设备安全

信息系统的硬件设备价格昂贵，一旦被损害将可能造成严重的后果和经济损失，因此必须加强对硬件设备的使用管理，坚持做好硬件设备的日志维护和保养工作。同时，计算机系统的各种电子设备工作时会受到电磁波干扰，当电磁干扰达到一定程度时就会影响设备的正常工作，因此要做好电磁兼容和电磁辐射的防护工作。

3）介质安全

系统的数据信息要存储在各种介质上，常用的介质有硬盘、磁盘、光盘、磁带、移动存储介质等，必须要做好介质的安全管理。移动存储介质常用于开放环境中，易于丢失，存储的数据易于传播和复制，自身缺乏有效的审计和监管手段，整个数据移动通道的安全保密工作难以保障。一旦发生数据泄露与丢失，将给部门或个人造成不可估量的经济损失，甚至可能是政治损失。因此，针对移动介质的安全解决方案是当务之急。

4）通信线路安全

通信线路的安全涉及电缆加压技术、光纤通信技术、Modem 通信安全等。

物理完全是相对的，在设计物理安全解决方案时，要综合考虑需要保护的硬件、软件及信息价值，从而采取适当的物理保护措施。

5.1.3 安全技术设计

安全技术体系能够在技术保障方面为信息系统提供深入全面的安全保护。信息系统的安全技术主要有两个研究领域：安全防护技术和安全管理技术。

1. 安全防护技术

安全防护技术是为保障信息系统稳定、正常运行，并防止外部入侵、攻击、破坏和窃取信息的防护技术。也就是狭义上的“安全技术”。安全防护技术包括物理安全技术和系统安全技术两大类。物理安全技术在 5.1.2 节有相关介绍。系统安全技术考虑的是信息系统和安全组件的操作系统的安全性，为了使信息系统安全组件所处的软件平台的安全等级达到相应的安全需求，需要考虑 3 方面因素：一是操作系统本身的脆弱性和漏洞引发的安全风险，主要包括身份认证、访问控制、系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。

同时，信息系统在建立的过程中应遵循多种安全防护技术标准，如图 5.1 所示。

2. 安全管理技术

协调信息系统各安全组件的操作与活动并完成安全保障任务所需要的组织管理技能称为安全管理技术。安全管理技术体系结构是要说明安全系统实现的技术指南和规则，包括安全服务和安全接口的技术规范。其相对应的安全技术视图的组成部件应该包括与安全系统相关的技术标准和规范。

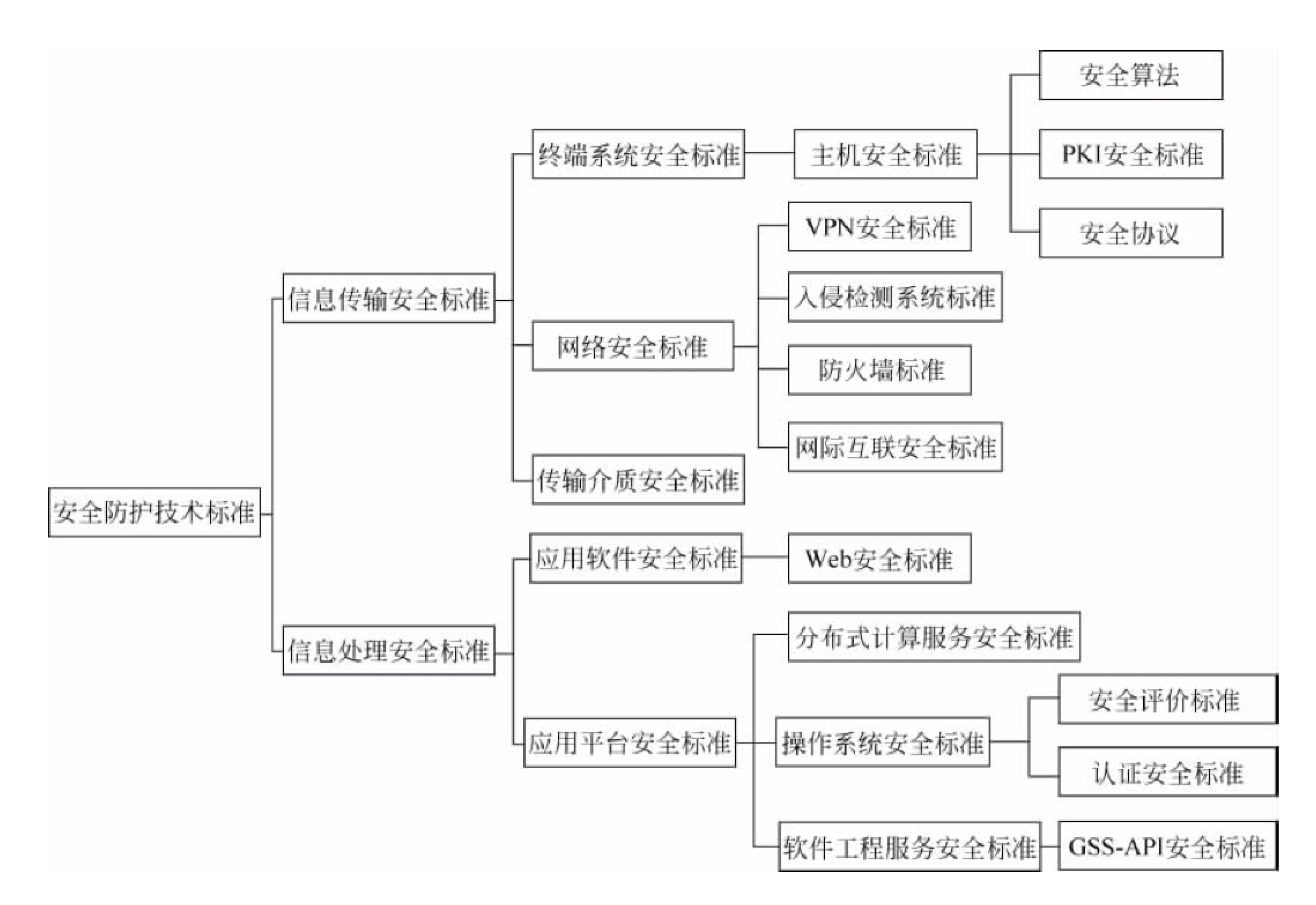


图 5.1　安全防护技术标准的层次结构

安全技术不仅是确定信息系统安全目标的重要因素，同时也是达到这些安全目标的具体实现手段。作为安全设计的重要依据，安全技术视图根据设计过程中可能遇到的工程或技术问题，明确系统安全风险，并增进安全技术的复用，方便系统的定义、批准、实现和改进，从而降低系统实现的成本。

安全技术视图的有效性和全面性直接影响到安全系统的互操作性和保障能力，是开发和维护安全系统的指导性文件。随着科技的进步与发展，新技术的不断涌现导致旧的技术逐渐被淘汰，安全技术呈现出很强的时效性。因此，安全技术视图的构建应该从时效性的角度出发，充分体现其时间特性。

为了能够清晰明了地设计信息系统的安全体系结构，系统地描述安全技术视图，下面给出了构建安全技术视图的基本步骤。

(1) 确定实施范围。

根据安全服务的设定、安全机制的选择、安全部件的设置以及安全管理操作的要求，确定安全技术视图的覆盖范围和涉及的安全技术种类。

(2) 选择技术标准。

针对各安全技术领域，选择应遵守的技术标准，用安全技术框架描述，注意应该选择国际通用的、成熟的技术标准。统一对相关术语的认识，尽量参照相关标准对术语的定义，可以用安全技术术语表描述。

(3) 预测发展趋势。

用安全技术预测的方法对相关领域的技术和标准的发展趋势进行预测，其中包括对现有技术或标准可能被淘汰的时间判断，对新技术或标准的可获得性预测，对某种标准的市场

认可度的判定,以及对预测结果可信度的描述。

(4) 描述技术指标。

用安全技术指标说明的方法对安全系统各组成部件的技术指标进行描述。安全技术指标的描述可以为系统部件的选购、开发、组合、管理以及更新和升级提供指导。

(5) 描述并评价安全技术视图。

结合以上几个步骤的设计,描述并评价安全技术视图,从而确定安全系统的技术水平以及进一步的改进方向。

5.2 信息安全工程系统设计

在开发信息系统功能体系结构和物理体系结构期间,ISSE 小组为客户提供安全性分析与建议。开发过程反复进行,涉及系统多个安全事件及安全工程生命周期的若干阶段。ISSE 小组根据客户提出的系统需求,并采用仿真、建模等技术,完成信息安全工程系统设计工作。

首先分析多种设计类型,以便将系统安全需求与各类安全服务相关联,然后再把这些安全服务映射到相应的安全机制中。然而,这样做对有些项目并不一定会有帮助,例如,有的项目要求开发新的应用软件或硬件,因此,“可重用性”的安全协议和机制将不再适用。在安全服务的实现阶段,系统体系结构的安全解决方案可以参考目标安全体系结构(Goal Security Architecture,GSA)。GSA 中可用的项目主题包括:

(1) 国防目标安全体系结构(DoD Goal Security Architecture,DGSA)安全需求——策略、需求以及导出的需求。

(2) 安全概念和安全角度。

(3) 安全管理概念和关系。

(4) 安全学说:能够提供安全服务的安全机制学说。

(5) 端系统和中继系统。

(6) 传输系统主题。

(7) 商业现货(Commercial-Off-The-Shelf,COTS)。

根据当前解决方案所存在的风险以及前期的经验教训,ISSE 小组重点对系统结构进行研究,识别当前体系结构所面临的威胁与脆弱性,并提出建议性的保护措施和可选择解决方案。

系统可以通过采用不同类型的安全机制或实现方法等保护措施来满足安全需求,同时,若两个以上的系统需要进行交互,那么一定要建立相应的交互规则和接口协议。当具有不同安全需求与策略的系统的运行受到限制时,或者新连接可能引起附加风险或与当前系统或基础设施发生冲突时,需要进行协商和折中分析以支持交互,尤其需要建立交互规则和接口协议。

系统开发完成之后再添加规划之外的防御措施或保护措施,一般很难实现与系统的理想结合,操作起来成本很高,并且不一定能达到预期的效果。然而,信息技术发展迅速导致信息系统安全需求随着时间变化很快,人们很难预先完全掌握系统的安全需求。因此,需要

建立一个可以进行开发并动态修改系统需求的基础体系结构。

用文档来形式化描述安全设计，并说明要满足的安全需求及理由。尽管在安全验证和风险评估过程中，都对信息系统进行了独立的分析与评价，但是对于包括 ISSE 参与者的系统设计小组来说，更重要的是系统地描述系统安全状态并将其列入系统设计文档，为设计评审提供指导。

ISSE 小组在任何时候都应当考虑采用新技术来满足安全需求的必要性，对于任何有希望使系统概念增值的安全新技术，ISSE 小组都必须对其进行调研，包括使用原型法进行系统的运行评估、应用、测试等，并预估使用新技术对信息系统造成的风险，并考虑降低安全风险等级的方法，确保能成功地将该项新技术集成到系统设计中去。

在系统开发早期，ISSE 小组可能仅仅关注需要什么技术，而不会事先识别出所需的基本关键技术。而在系统生命周期的设计、实施以及后续生产或修改过程中，预先识别并建立起基本关键技术是非常重要的。为了满足特殊安全需求所需要开发的新技术，需要给予足够的时间来保证该项技术的研究与开发，同时还要保证其他工作项目的进度，不能与客户要求的进度发生冲突。ISSE 小组必须要保证采用新技术的收益大于由于依赖该技术所带来的风险和增加的成本。一般情况下，采用新技术或新产品所产生的依赖将会对整个技术带来额外的费用和技术风险，并且有可能影响项目实施进度。因此，必须仔细并长期监控这些新技术或新产品。将新技术加入系统计划之前，ISSE 小组应该将其带来的所有风险和潜在利益告知客户，并准备好后备产品和解决方案，以便及时处理由于使用新技术或新产品所带来的技术问题或偶然事故。例如，某些新的密码算法的研究与开发以及安全性评估需要花费大量的时间与费用，因此会影响到系统的进度与成本。

ISSE 小组要明确系统设计中影响和限制所需安全服务实现的约束因素，许多因素都会对诸如系统的设计过程或系统如何满足其安全需求等造成约束，如系统的运行模式（分级模式、专用模式或高层模式）、运行环境、业务功能等因素都可能对系统设计造成约束。互操作性和接口特性也可能是影响设计的约束因素。系统设计及运行的安全状况也可能受到某些支持性需求的约束，这些需求包括生存性需求、可移植性需求、后勤支持需求、情报和通信接口需求、标准化和互操作需求等。

随着系统设计活动的不断推进，ISSE 小组还需要将由于设计的选择而引出的新安全需求向需求定义函数做出反馈，并将其准确定位到可追踪体系与决策数据库中。例如，系统选择数据高度机密保护方案，那么可能要求将保护数据抗篡改作为附加需求。

在系统工程周期内，ISSE 小组将通过培训、支持、运行以及其他系统工程功能的并发应用，开发系统设计规划。同时，深入研究学习开发活动，进而评估系统安全解决方案的有效性和适用性。

为满足安全需求，ISSE 小组应该从技术和非技术两个方面进行考虑。例如，为某信息提供机密性保护，可以采用加密技术来满足其安全需求，也可以采用非技术性解决方案，如信息隐藏或其他物理手段。技术性解决方案在安全技术设计中已经一一做了介绍。非技术性解决方案包括过程控制（如人事及操作程序的安全控制）和可信软件开发方法论（Trusted Software Development Methodology，TSDM）中的非技术要素等。

5.3 生命周期安全设计

信息系统安全的生命周期包括任务阶段、概念阶段、需求阶段、系统设计阶段、配置审计阶段、运行与维护阶段。从系统工程的角度分析，信息系统安全设计应涵盖对生命周期各阶段的安全分析与设计。

5.3.1 任务阶段的安全设计

任务阶段的目的是确定系统所要完成的任务，通过对任务需求的考察与分析，确定信息系统所应具备的安全能力，并提出可选方案。该阶段很少用到安全设计活动，但在准备进行备选系统评审（Alternative System Review，ASR）时，系统工程和 ISSE 小组应该开发若干个备选的系统设计。这些备选方案是由过程和产品解决方案相互融合产生，每个备选方案都应与 MNS 业务需求说明中所描述的高级业务能力保持一致。

5.3.2 概念阶段的安全设计

为了完成进一步的开发与设计，需要选择最好的系统方法进行备选系统评审。为了支持 ASR 时的决策，系统工程必须对每一个概念级备选方案进行充分分析，并提炼出安全体系结构，为备选方案准备一组可行的系统运行需求。早期，通常由不成熟的功能结构体系和物理结构体系草案构成概念级系统策略。由于项目所处环境的不同，概念级设计可能很不正规，也可能非常完善。但无论概念级设计是否完美，由于在系统设计阶段需要提交一份待批准的设计文件，因此该阶段所承担的设计等级要低得多。

系统工程师将对在开发体系结构的备选方案进行反复比较并完成折中分析。同时，ISSE 小组必须要确保所开发的体系结构已经足够精细，才能够保证安全风险评估进展顺利，并支持 ASR。

ISSE 小组应该将系统功能分解，并将其配置调整到较低级别上，直到支持当前正在进行的评审分析，满足 ASR 的决策要求。如果选择自动化工具并使用得当，将会得到事半功倍的效果。ISSE 小组在选择方法论和工具时的原则是：首先考虑并遵循客户意见；如若不行，就考虑上级机构的建议。

5.3.3 需求阶段的安全设计

需求阶段的目的是分析安全需求和研究安全需求概念。根据提交的安全需求说明书进行审核。系统工程小组在需求阶段完成系统的高层设计，并形成符合技术规划的设计文档。随着系统功能评审（System Functional Review，SFR）的结束，系统设计的基线也随之完成并被批准，此时，应该审核与备选策略一致的结构体系方案。例如，假如经过评审后的概念阶段选择了广域网策略，那么在需求阶段将会选择广域网技术并对其体系结构进行取舍。

任务阶段及概念阶段的安全设计活动在需求阶段仍然要继续进行，继续分解功能体系结构和物理体系结构，直到分解成重要的组成单元，以便决定是制造还是购买。ISSE 小组应该保持安全服务的强度，不能因为支持这些安全服务的配置就将其功能强度削弱。

5.3.4　系统设计阶段的安全设计

系统设计阶段包含两个部分的内容：概要设计和详细设计。概要设计的目的是确定顶层安全体系结构，并根据提交的安全需求功能说明书进行审核。而详细设计阶段的安全设计最为复杂，是信息系统安全性设计成功与否的关键。

系统设计阶段的早期就要进行系统集成，当功能需求部署到配置项目 CI 上时，要用到接口控制规范。ISSE 小组应该在接口控制规范中指出这些接口实现安全服务的方法，安全服务应当包括扩展的基础设施和业务环境。例如定义接口协议、制定标签体系结构的标准等。如果系统与网络基础设施相连接，那么网络环境中所用到的体系结构将会对安全需求造成约束。通过指定内部和外部接口的安全需求，系统与互连的其他系统之间能够在实现上保持一致，有利于集成业务的完成与实现。ISSE 小组还要验证系统组件，并根据组件与安全接口的约束条件进行集成和使用。

通常由基于可推荐产品的层次体系来决定 CI 是制造还是购买获得，该层次体系的范围从优先推荐使用商业销售与支持的软硬件产品起，不断降低为使用政府现货（Government Off-The-Shelf，GOTS）项目，再到修改的项目，直到定制开发的项目。工程项目的开发多是针对实际应用，很少有项目不做任何针对应用的开发。

要做出是制造还是购买的决策，折中分析必不可少。在进行折中分析时，ISSE 小组必须要保证所有安全因素都被包括到总体分析中，并确保体系结构全面而且各项功能、特性、费用、进度和风险之间的协调平衡。如果所描述的功能保障等级是由不成熟的 CI 所提供，那么就应当考虑购买而非制造。如果通过折中分析以后做出定制开发的决策，那么需要考虑包括制造环境和装运过程在内的各种因素，以保证不降低预期的保障等级。根据要开发的 CI 的敏感等级，选择合适的制造者。

在系统设计阶段，将提出制造或购买的建议。但是，通常会在过程结束之后才做出最终决定。因为在此之前，ISSE 小组还要为在折中分析期间未包含的负面因素提供解决方案。例如，如果折中分析得出的决策是购买商用软件，但该软件可能会包含潜在的病毒，这是一个很重大的负面因素。在软件购进以后，ISSE 小组可提出进行病毒扫描和清除的建议，以减少由购买软件所带来的安全风险。

ISSE 小组将对现有产品进行调查分析以确定其是否满足组件或 CI 的需求，从而对折中分析的决策做出支持。调查分析的对象包括信息系统安全产品目录、可信产品评估目录、供应商产品目录、信息系统安全知识库等。如果系统允许，那么一定要制定一组可行的备选方案，而不应该仅仅提供一个候选方案。对于政府或工业界先期开发的新产品和新技术，如果它们所带来的技术风险及其时间表是系统开发可以接受的，那么 ISSE 小组也要考虑使用。

工程师在做出制造或购买决策时，要对产品的安全需求进行描述，形成安全评估报告。为了做出准确的 ISSE 制造或购买决策，对现有产品的了解与认知必不可少。对于某些产品，有关部门的安全评估报告有助于决策的形成，安全评估报告涵盖了产品的功能、使用信息以及产品的脆弱性。对于不能进行安全评估的新技术，系统项目办事机构（SPO）会将新软件或设备与预估的风险相关值和安全特性进行权衡比较，从而做出是购买还是定制的决策。

5.3.5　配置审计阶段的安全设计

配置审计阶段的主要任务是评估并更新系统安全威胁，预测系统的使用寿命，找出安全

方案实现后系统和配置项的安全需求和限制。同时跟踪与本阶段相关的安全保证机制,进行安全风险评估。此外,配置审计阶段还要对系统进行安全测试,提交系统安全测试、配置和验证说明书。

最终的购买或定制的决策必须要通过系统工程师的初步设计评审(Preliminary Design Review,PDR)以及对 CI 之间接口策略的备用方案的反复研究做出。以前的活动集中在 CI 的设计或选择以及完整的 CI 级配置基线集的建立上,该阶段宣告结束的标志是系统验证评审和配置审计的成功实现。以后阶段的活动则集中于 CI 集成测试系统的建立与获取上。

CI 集成开发与测试时对系统设计所做出的任何修改,ISSE 小组都应当进行审查。一旦 CI 引起系统的附加需求,ISSE 小组就应该评估其影响并更新系统设计以满足附加安全需求。例如,当系统选择其他有优势的 COTS 时,从安全的角度来看,可能存在一些脆弱的行为和特性,并且会影响到其他系统过程解决方案或 CI 产品的安全需求,因此需要增加附加安全需求。对于 SPO 支持的相关 CI 技术,ISSE 小组应当进行审查,并对其进行信息系统安全分析,当集成为整体系统时,要保证 CI 满足安全需求。

5.3.6 运行与维护阶段的安全设计

运行与维护阶段要实施安全操作和生命周期支持,以保证安全级别在系统运行期间不会下降。在系统运行与维护阶段内,为了方便提出适合系统修改的设计方案以及对预定计划的改进措施,要反复进行安全设计活动,并进一步讨论系统修改问题。

5.4 本章小结

本章主要介绍了信息系统安全设计活动,安全体系结构描述了信息系统的安全机制、安全服务、安全特性以及满足安全需求的各基本要素之间的关系,安全设计则提供了对那些满足系统需求的安全服务、安全机制和安全特性的深刻理解。本章从安全体系结构和信息系统安全生命周期两个角度,分别对信息系统安全设计做出分析。首先分析系统安全体系结构,信息系统安全设计包括对安全系统、安全功能及安全技术 3 方面的安全设计。最后分析生命周期的各阶段的安全设计活动,包括任务阶段、概念阶段、需求阶段、系统设计阶段、配置审计阶段以及运行与维护阶段的安全设计活动。

5.5 习题

1. 简述信息系统安全设计的意义。
2. 简述安全体系结构设计过程。
3. 简述系统设计的功能实现。
4. 安全技术设计包括哪些方面?
5. 通过学习本章的内容,简要介绍信息系统生命周期安全设计。

第 6 章　信息系统的安全性测试

信息系统是一个复杂系统，它由众多部件构成，其安全测试存在着很大的挑战。目前，国内外已有比较成熟的关于安全产品的测试评估的标准及方法。与安全产品的测试不同，信息系统的安全性测试都还处于探索阶段，国内外有许多安全组织和机构都在积极地研究信息系统安全测试的方法和实践，但仍然没有形成比较统一的测试标准。在信息系统安全评估方面我国已有一些标准和指南，但在信息系统安全性测试方面仍然缺乏相应的规范和标准。国外关于信息系统安全测试的公开文献都缺乏对安全测试的整体研究。

6.1　信息系统测试概述

系统测试是这样一个过程，它为了发现程序中的错误而执行程序。系统测试横跨系统生命周期中的两个阶段。一般情况下，系统的每个模块在编写出之后需要对其进行必要的测试，称为单元测试。模块的编写者和测试者是同一个人，编码和单元测试属于系统生命周期的同一阶段。在此阶段结束之后，还要对软件系统进行各种综合测试，综合测试通常由专门的测试人员来完成，它属于系统生命周期的另一个独立的阶段。

6.1.1　测试目标

根据立场的不同，测试存在着两种完全不同的目的。一种是从系统开发者的角度出发，希望测试能够证明系统产品中不存在错误，验证该系统已正确地实现了用户的要求，确立用户对系统质量的满意度。另一种是从用户的角度出发，希望通过系统测试能够检查系统中是否存在潜在的或隐藏的错误或缺陷，以考虑是否可接受该产品。

Grenford J. Myers 对系统测试的目的提出以下观点：

（1）测试目的是发现系统的错误，它是程序的执行过程。

（2）一个好的测试方案是能发现至今尚未发现的错误的测试方案。

（3）一个成功的测试是能够发现至今未发现的错误的测试。

总体来说，测试目标是希望以最少的时间和人力，发现系统中潜在的各种错误和缺陷。

系统测试的主要任务包括：代码漏洞测试、功能测试、性能测试、故障诊断及问题定位、文档评审。

（1）代码漏洞测试。

扫描系统的源代码，查找系统的安全漏洞。

（2）功能测试。

① 验证系统的基本功能是否正确。

② 验证系统的功能实现是否完整和满足需求文档中的要求。

③ 验证系统的可靠性、易用性、可移植性和维护性等。

④ 验证系统的内外部接口功能是否正确实现。

(3) 性能测试。

性能测试模拟大量并发用户的活动,重复运行测试,发现系统在重负载下受到的影响,确认性能瓶颈,从而对系统进行优化和调整。

(4) 故障诊断及问题定位。

根据用户、测试和集成商等发现的问题,对整个系统的相关运行数据进行整理,分析采集结果,定位出问题发生的具体位置,以便系统开发方进行修改,针对问题进行回归测试。

(5) 文档评审。

对系统开发方在项目实施过程中的可行性研究报告、项目规划、需求分析、概要设计、详细设计、用户说明等相关文档进行评审,验证是否包含了国家标准中关于系统设计文档的主要测试指标。

6.1.2 测试原则

系统测试是一项非常复杂的任务。下面列出了测试时的主要原则:

(1) 应尽早地和不断地进行系统测试。

(2) 测试工作应避免由原开发机构进行,单元测试除外。

(3) 设计测试用例时,要包括合法的输入数据的和非法的输入数据。

(4) 设计测试时要确定输入数据及与之对应的预期输出结果。

(5) 充分注意测试过程中的群集现象。

(6) 严格按照测试计划进行,避免测试的随意性。

(7) 对所有的测试结果做全面检查。

(8) 检查程序是否做了应做的事和不应做的事。

(9) 对修改的程序进行回归测试。

(10) 保留测试计划、全部测试用例、出错统计和最终分析报告,作为系统文档的组成部分。

6.1.3 可测试性

1. 可测试性概念基础

可测试性的概念最早在航空电子领域产生,由 F. Liour 等人于 1976 年在《设备自动测试性设计》一文中最先提出。当时,由于一些硬件电路系统膨胀到一定的数量级,对其进行测试就显得异常复杂,众多研究人员就提出了针对硬件电路的可测试性度量方法,形成了硬件测试的一个重要分支——可测试性分析。随后,美国国防部相继颁布了 MIL-STD-471A 通告 II——《设备或系统的机内测试、外部测试、故障隔离和可测试性特性要求的验证及评价》、MIL-STD-470A——《系统及设备维修性管理大纲》和 MIL-STD-2165——《电子系统及设备的可测试性大纲》等一系列与可测试性相关的标准和规范。其中,《电子系统及设备的可测试性大纲》规定了可测试性管理、分析、设计与验证的要求和实施方法,标志着可测试性从维修性分离出来,成为一门独立的新学科。

可测试性是指产品能及时准确地确定其状态,隔离其内部故障的设计特性,状态包括可工作、不可工作和性能下降等。以提高可测试性为目的进行的设计被称为可测试性设计。

可测试性描述了测试信息获取的难易程度，它和可靠性一样，也是设备本身所固有的一种设计特性。可测试性的关键技术包括：

(1) 可测试性度量。

(2) 可测试性机制的设计与优化。

(3) 测试信息的处理与故障诊断。

可测试性工作的目标是确保系统和设备达到规定的可测试性要求，提高系统和设备的完好性，保证任务成功，减少对维修人力和其他资源的要求，降低生命周期费用，并为管理提供必要的信息。具体目标包括：

(1) 设计完善的 BIT(Build In Test)，提高系统的可靠性和安全性。

(2) 自动、快速地检测和隔离故障，提高系统的可靠性。

(3) 通过 BIT、外部测试及兼容性设计，降低系统的复杂性，减少信息保障费用，降低生命周期费用。

系统或设备的可测试性工作对于提高设备的可靠性和维修性是非常重要的，可测试性工作的具体内容包括：

(1) 确定诊断方案和可测试性要求。

确定并评审诊断方案，提出能最好地满足诊断方案的系统可测试性要求。

(2) 制定可测试性工作计划。

明确要求的工作项目并进行合理的安排，以达到规定的可测试性要求。

(3) 可测试性初步设计和分析。

在设计早期，把可测试性设计到系统和设备中，并评价其程度。

(4) 可测试性详细设计和分析。

把可测试性设计到系统和设备中去，评价系统和设备可能达到的可测试性水平，保证可测试性能有效地综合和兼容其他诊断要素。

(5) 评审可测试性工作。

及时评审可测试性工作，保证可测试性工作按要求和计划进行。

(6) 验证可测试性要求。

验证系统和设备是否满足规定的可测试性要求，并评价可测试性的有效性。

(7) 制定可测试性数据收集和分析计划。

对生产和使用过程中与可测试性有关的问题进行检查，并确定其纠正措施。

2. 软件可测试性

信息系统的可测试性包括硬件可测试性和软件可测试性。

硬件可测试性分析是指对一个已初步完成设计的电路或者待测电路，不具体生成测试码就能定量地估算出电路测试难度的一类方法。它有两个基本要求：

(1) 准确性。

准确性是指对电路的可控制性、可观察性和可测试性的相对大小关系能真实描述故障检测的难易。

(2) 易计算性。

易计算性是指可测试性分析方法的计算复杂性远远低于测试生成，否则将失去其存在价值。

到了20世纪90年代,研究人员逐渐把硬件的可测试性分析研究应用到软件上,软件可测试性研究成为关注的焦点。软件可测试性概念的解释最早由1990年的IEEE STD. 610.12中给出。软件可测试性作为软件的一种质量特性,并没有一个统一的定义,Freedman在1991年提出把可测试性定义为可控制性和可观测性的集合。可控制性是指便于对产品的内部状态进行控制,可观测性是指能够对产品的内部状态进行观测。随着时间推移,软件可测试性概念不断完善,研究者根据各自研究的初衷,对软件可测试性给予了不同的定义。以下是3种对软件可测试性的定义。

1) IEEE(1990)标准

(1) 为一个系统或构件建立测试标准,并通过执行测试来确定该标准被满足的难易程度。

(2) 对每一个声明的需求建立一个测试标准,并通过执行测试来确定该标准被满足的难易程度。

2) ST Lab 标准

一个软件能够被测试的有效程度的判断。

3) Jeffrey Voas 标准

软件中存在错误,它在下一次被测试执行时产生故障的概率。

此外,更一般的软件可测试性定义是软件中存在的错误在给定任意输入集合的测试过程中被揭示出来的概率。

总的来说,软件可测试性实质是对软件进行有效测试的难易程度的一个指标,但是该指标没有对可测试性进行量化。对可测试性进行量化研究,可以直观地判断不同软件可测试性的好坏,增强可比性,合理分配测试资源,提高测试效率,评价软件测试难易程度也会更加方便。此外,该量化指标也可用于评估软件的可靠性度量和可测试性设计。

国际上对软件可测试性的研究至今已有10多年,并从不同角度提出了分析和检测软件可测试性的方法。根据实现的方式,这些方法可以分为两大类:

(1) 用静态分析的方法来检测,如基于数据流分析的可测试性度量、PIE模型静态实现、静态程序可测试性分析模型等。静态方法多为基于概要、详细设计或者对程序代码的静态结构分析,依据一定的规则,实现对程序的可测试性分析。这类模型适合于设计阶段的验收测试。

(2) 用动态执行的方法来检测,如PIE模型、语义故障模型等。动态方法强调动态运行被测程序,通过插入和安装程序变异因子的方法观察其对程序执行过程和输出的影响,进而评估程序的可测试性。这类模型适合于单元和集成测试阶段对软件进行的白盒测试。

国内对软件可测试性的研究起步比较晚,从已有的文献来看,主要着重于对软件可测试性进行定性研究或者可测试性设计策略的制定上,并没有提出新的软件可测试性检测的解决方法。

目前,关于软件可测试性的研究已经越来越多,研究的内容范围也越来越广泛,其研究成果也可用于指导测试资源的合理分配、软件设计模式改进和软件可靠性模型建立等方面。

3. 软件的可测试性的特征

软件可测试性具有以下特征。

1）可操作性

软件存在很少错误或基本没有错误的话，软件运行得很好，在进行测试时的效率就会很高。

2）可控制性

能够从软件的输入来控制它的各种输出，软件硬件状态和变量可由测试工程师直接控制，软件的自动测试工作变得更容易。

3）可观测性

可观测性好的软件产品可以容易地观测到想测试的东西。

4）可分解性

软件可被分解为多个独立的模块，每个模块都能进行独立测试。

5）简单性

要求软件在满足需求的基础上尽量简单。

6）稳定性

软件保持稳定的状态，变化很少。

7）易理解性

软件的设计易于理解。

4. 软件可测试性研究意义

软件的可测试性是一个软件度量指标，它的高低决定了测试该软件进行的难易程度，即软件中的错误被揭示出来的可能性。可测试性分析可用于指导软件设计人员合理地设计软件结构，降低测试的开销并提高测试的可行性。改善了软件结构，也能直接避免一些软件中的错误，使软件的可靠性和可信度达到较高的水平。对软件可测试性分析的研究，有助于确定软件为了达到一定的可靠性而需要被测试的程度，并提高测试的覆盖率。由于软件测试的固有的复杂性，使得软件开发中测试的成本越来越高，但软件的可靠性仍未得到保证。分析研究软件可测试性的目的是将其应用在软件质量保证中，合理分配资源，减轻测试工作量，提高软件的可靠性。研究软件可测试性及其量化方法对评价软件测试难易程度和对软件的测试、软件的质量保证以及改进软件结构设计都具有一定的指导意义。

5. 软件可测试性分析方法

根据可测试性的不同定义，可以有多种可测试性的分析方法，并且不同的方法针对不同的软件属性。由于软件之间的结构、设计方法、设计层面以及测试方法等的差异，将可测试性分析方法分为多个种类。比较典型的 4 类大致归纳如下：

第一类，此类的主体思想是基于某种流图，对图中各种结构信息（如点、边、路径数、循环数等）进行统计计算。这些信息的统计不依赖于程序的执行和测试策略，而是以模块为单位，得出的结果可用于比较不同的程序结构的优劣，找出软件中的需要重点测试的位置，指导软件的改进。Jin-Cherng Lin 和 Pu-Lin Yeh 提出的基于数据流的方法、宫云战等提出的基于程序流图的方法和 Taghi M. Khoshgoftaar 等人提出的基于神经网络的方法都属于这一类。

第二类，基于信息论的分析方法，主要由 Robach 等人提出。此类方法基于信息流图，以模块的输入和输出信息为依据，对可控制性和可观测性进行定量计算，从而确定其可测

试性。

第三类,以 PIE(Propagation analysis,Infection analysis and Execution analysis) 技术为基本原型,针对程序中的某一位置进行分析,计算在该处故障能被检测到的概率。对程序中关键语句进行分析,结果可用来指导相应的测试工作,从而节省资源,提高测试效率。

第四类,基于 UML 类图的分析技术。此类方法主要以 UML 类图为分析对象,发现构件中类之间的复杂依赖关系并进行消除,提高软件的可测试性。

除了上述几类方法外,也可从其他角度对软件可测试性进行分析。

软件可测试性分析通过对软件自身结构的量化分析,从而指导软件测试的分析。在软件的分析和设计阶段开始软件可测试性分析,能及时地发现软件中存在的不合理结构,或者是不利于软件测试的结构,从而作出针对性的调整。

6.1.4 信息系统安全测试框架

在对一个复杂的信息系统进行安全测试时,需要分析和考虑多方面的内容,具体包括如下几个方面。

1. 制定安全测试策略

在综合考虑测试目的、成本与效益、风险控制等要素基础上,制定测试活动相应的安全策略。制定安全测试策略的目的是指导安全测试方法和安全测试工程的实践,解决有关测试的原则性问题。

2. 全面剖析被测试信息系统

分析目标系统,确定安全测试的内容和方法,以及测试系统的安全性质的方法,确切、完整地反映出信息系统当前的安全状态。

3. 确定信息系统安全测试的技术和工具

信息系统的安全性涉及的范围很广,需要不同的安全测试技术和工具。另外,还要建立一个信息系统安全技术知识库,知识库需要包括安全漏洞库、病毒、蠕虫和木马特征库等。

4. 制定规范的安全测试工程

安全测试工程包括系统分析、测试计划、测试流程、测试记录和测试质量保证等方面。系统分析是指对被测系统和其安全性架构进行分析;测试计划包括安全测试的范围、对象、项目及其子项;测试流程是指信息系统安全测试的步骤;测试记录是指对安全测试的过程和结果进行记录和分析研究,形成安全测试报告。测试质量保证是指对安全测试进行管理控制和审查核实,以保证测试的公正性、真实性和可重复性等。

如图 6.1 所示是一种信息系统安全测试框架。

6.1.5 信息系统安全测试方法

安全测试可分为两种:静态安全性测试和动态安全性测试。静态安全性测试主要分析信息系统的架构、所采用协议及软件系统的设计和实现过程中的缺陷;动态安全性测试主要检测信息系统运行期间所表现出的安全脆弱性,安全脆弱性是指信息系统前期的设计、实施以及运行期间各种因素综合作用的结果。

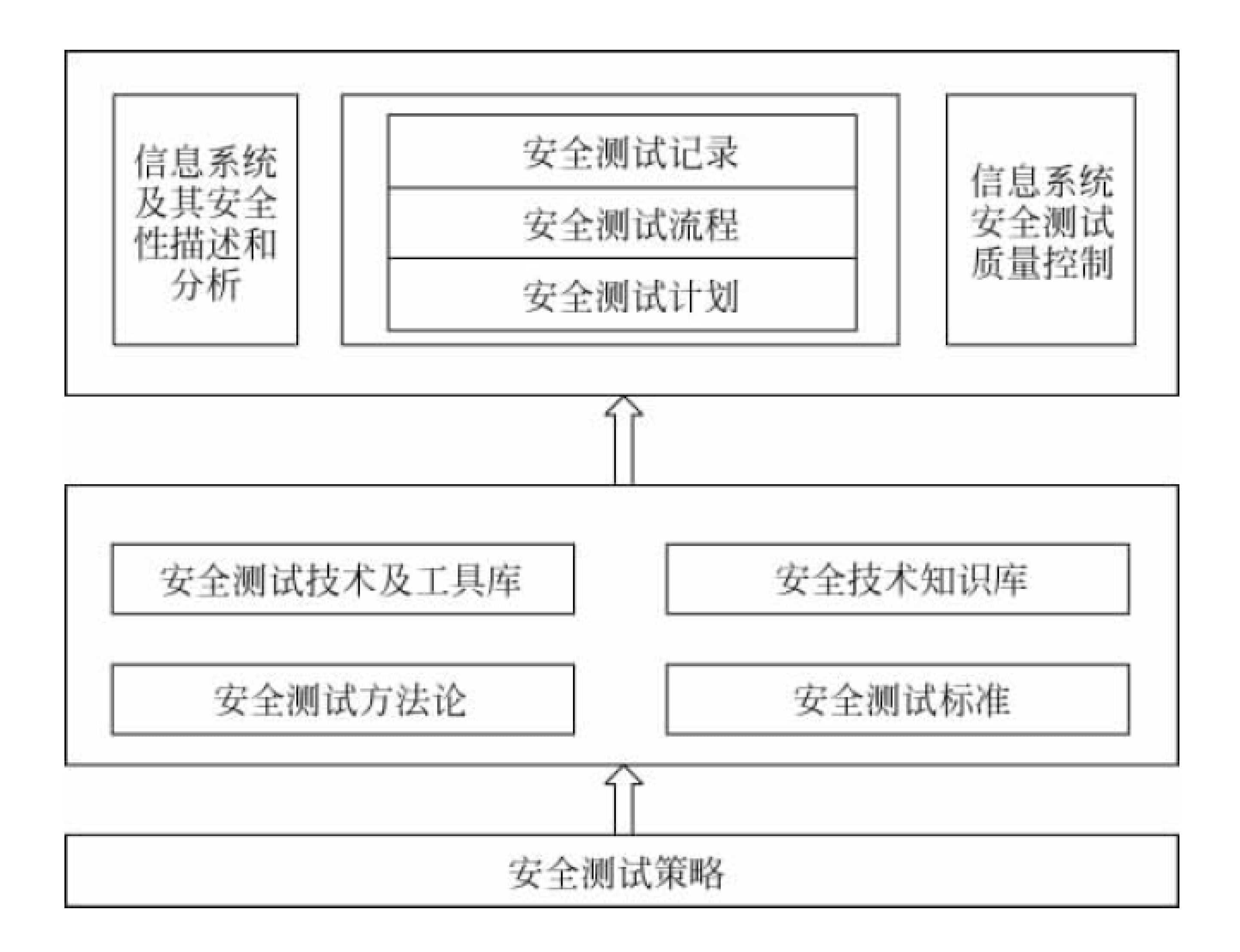


图 6.1　信息系统安全测试框架

1. 静态安全性测试

静态安全性测试侧重于软件安全性的测试，测试软件的设计和实现问题不会引起软件自身的问题，也不会影响其他或整个信息系统的安全问题。静态软件安全性测试是信息系统安全性的基础性和支撑性的安全控制措施。静态安全性测试通常是在信息系统的设计和实现过程中采用，而对已建成并运行的信息系统一般很少采用。静态安全性测试方法主要包括 3 个方面的内容：

(1) 审核软件系统设计的原则和架构。

(2) 分析和测试协议安全性。

(3) 测试软件系统源代码。

2. 动态安全性测试

动态安全性测试主要对运行信息系统的安全性进行测试，测试的目的是发现信息系统当前的漏洞以及潜在的脆弱性。动态安全性测试可采取 2 种方法：

(1) 从网络协议层角度，针对网络的整个协议层进行安全测试，实现整个网络协议层的纵深安全测试。

(2) 从网络拓扑结构角度，选择具有代表性的测试点对信息系统进行多方位的安全测试，实现对整个信息系统的全方位安全测试。

6.2　硬件安全性测试

计算平台越来越多地部署在许多重要的基础设施中，如智能电网、金融系统、敏感的政府组织等，一个成功的安全攻击造成的后果十分严重。因此，高风险领域的计算机平台的应用，推动了更高的安全平台的建立。但是，由于两个新出现的趋势，增加了加强安全平台建设的复杂性。

由于经济、社会和技术力量的影响，硬件安全已经成为首要的设计和制造目标。硬件安全涵盖了广泛的研究和发展方向，包括知识产权保护、硬件计量、硬件的特洛伊木马检测、安全的智能卡设计和物理容器使用电子锁的保护等。最近，硬件安全集成和评价工具的发展受到了极大的关注。然而，关于硬件安全方面的课程还没有被引入计算机工程课程。

面向硬件的攻击：计算平台包括一个软件栈，包括用户应用程序，操作系统和设备驱动程序，在一个包括处理器、芯片组、内存和外设的硬件上执行。此前，安全攻击主要是针对软件堆栈，并利用软件的漏洞，如缓冲区溢出、格式串等，以获得执行攻击者的恶意代码的权限。最近，安全攻击已经趋向于硬件，恶意操纵硬件的设置，以方便绕过硬件保护机制。在一个平台上，硬件是最有特权的实体，操纵它有可能给攻击者相当大的灵活性和权力发动恶意安全攻击的能力。此外，许多面向硬件的攻击有能力逃脱以操作系统为基础的机制，如防病毒扫描的检测。

1. 硬件组织基础

一个计算平台的硬件由许多元件相互交融，实现平台功能。一个典型的计算平台的硬件组织包括 3 个主要部分，即集成电路芯片、外设接口和总线。每个硬件类型的功能和举例说明如下。

1）集成电路芯片

这些芯片实现逻辑控制，数据处理和存储固件代码执行。除了中央处理器，其他的芯片，如内存控制集线器（Memory Controller Hub，MCH），调节 CPU 和外设的访问内存；输入/输出控制器（Input/Output Controller Hub，ICH），调节 CPU 和不同的外围设备之间的访问；动态随机存取存储器（Dynamic Random Access Memory，DRAM），实现存储；可编程中断控制器（Programmable Interrupt Controller，PIC）；可信平台模块（Trusted Platform Module，TPM），实现加密功能；存储 BIOS 固件和嵌入式控制器（Embedded Controller，EC）的监管平台等。通常情况下，MCH 和 ICH 都统称为芯片组。因此，除了 CPU，有多个芯片控制平台的信息流，影响整体平台的安全。

2）外设接口

这些电气接口是负责实施底层外围设备连接到平台的各种标准的通信协议。这种接口包括 USB 接口、SATA（例如，硬盘驱动器）、PCI、LPC（例如，TPM 设备）和 GBE（例如，有线和无线网卡）。

3）总线

总线负责芯片和外设之间数据传输。著名的例子包括 CPU 和 MCH 和直接媒体接口（Direct Media Interface，DMI）总线之间前端总线（FSB），连接 MCH 和 ICH。

2. 硬件的安全隐患

图 6.2 表示了一个 IC 设计模型。

该木马可以通过主总线上的一个特殊的值被激活，例如，它可以存储目标数据的地址。一旦木马电路被触发，有效载荷可以是下列之一：禁用系统，通过嵌入式接口将有用的数据传送给第三方，为进一步利用收集内存访问的信息，上升为当前系统中正在运行的进程的安全特权。

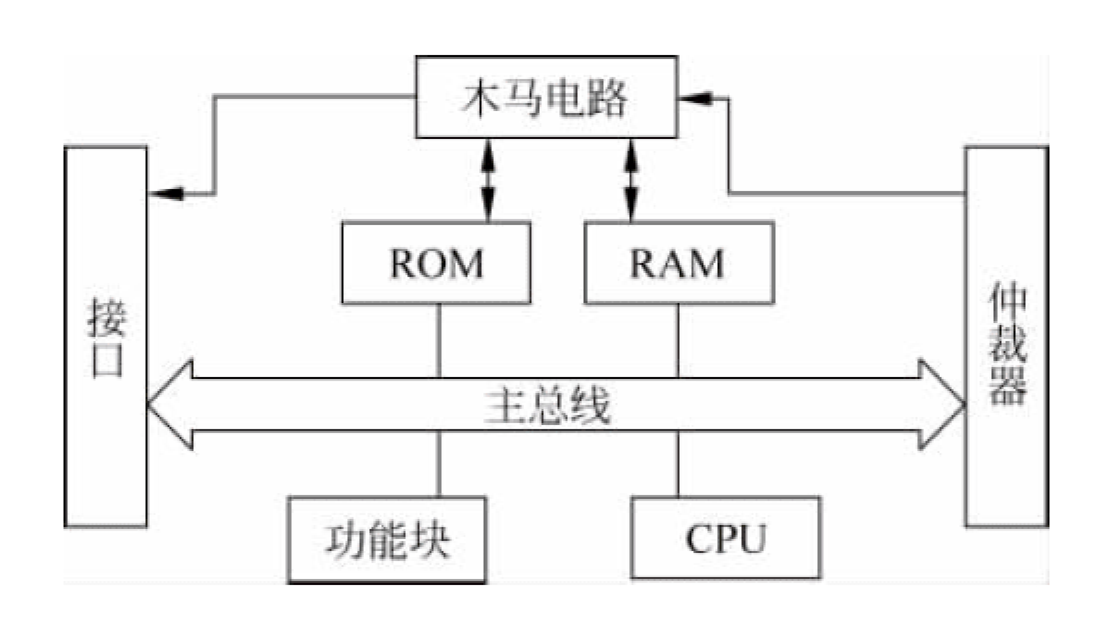


图 6.2　木马电路嵌入

3. 硬件攻击的类型

在硬件级别，每个 IC 芯片有大量的状态元素，芯片之间和外设接口通过互连总线发送的众多的控制信号相互交互。在此背景下，我们定义硬件安全漏洞为状态值和控制信号的特定组合，这将导致违反安全目标或绕过一个平台的访问控制机制。面向硬件的攻击者的攻击能够利用硬件漏洞威胁一个计算平台的安全。在硬件攻击已经被观察到，在实践中发生的方式的基础上，将其分为以下几种类型：

(1) 积极的对抗性的硬件控制信号操纵。

这一类的攻击，敌手积极操作平台上的控制信号，以破坏平台的访问控制机制。这些攻击可能需要附加 MOD 芯片或探头的到平台的物理访问，以影响硬件控制信号。

(2) 在多平台功能的互动安全性的缺口。

整个平台的功能，是通过在不同的平台组件功能集合实现的。然而，两个或更多的功能交互，可以创建被攻击者破坏硬件内置的保护的安全漏洞。由于平台上的状态和控制信号的指数，找出所有可能导致潜在的利用漏洞的相互作用是相当困难的。

(3) 不安全开机固件平台初始化。

硬件需要为正常的平台操作进行正确配置，初始化通过平台的引导固件完成，如 BIOS。BIOS 负责内存控制器的配置，它转换物理地址，由页表输出到 DRAM 芯片所需的索引位置的参数组合。如果配置不正确的内存控制器，然后基于页面的访问控制可能被绕过。因此，BIOS 在硬件平台的安全性起着不可或缺的作用。

(4) 不可信或规模较小的恶意影响硬件操作的特权实体。

和特权的平台实体——硬件一起，具有不同权限或信任级别的其他实体展现在平台上。当敌手能够利用平台上的一个较小的特权或不受信的实体，恶意影响硬件实施保护机制的运作时，整个平台的安全受到威胁。

在硬件接口方面，存在一些不同的安全隐患，可以进行以下测试。

(1) 串行接口测试：信息系统的串行通信的主要安全问题是抗干扰能力弱。串行通信协议要求在数据发送和接收之间采用统一的采样率，如果攻击者干扰传输通道，它可能会导致数据的校验错误，导致数据帧的丢失。此外，如果串行端口使用 RS-422 或 RS-485 标准，当信道遇到了强烈的信号干扰时，共模干扰会发生。这可能会导致接收器的输入电压超出正常范围，并在输电线路产生干扰电流，从而影响正常通信，甚至严重损坏通信接口电路。

(2) CAN 总线接口测试：在信息系统中，CAN 总线通信的主要安全问题是缓冲区溢

出。根据CAN接口通信协议，发送者需要建立标准帧，根据接收方的要求定义帧头、帧尾和校验。发件者还需要定义接收帧缓冲区的长度。如果发送帧大大超过缓冲区的大小，CAN接口的接收方无法接收正确的帧，可能导致缓冲区溢出。

(3) AD接口测试：AD卡是高速数据采集卡，AD通信的主要安全问题可能存在于以下几个方面：首先是输入电压的问题。AD数据采集卡的输入电压都有一定的范围，如果输入电压超过过载电压，过度加载的电压将烧毁采集卡，设备将停止工作。其次，当使用外部触发模式模拟数字的转换，采样频率取决于外部触发源，如果攻击者设置外部触发频率过高，AD卡写入到FIFO缓冲区的数据过快，导致缓冲区溢出和传入的数据丢失，降低了系统的信号采集能力。

(4) DIO接口测试：DIO的优势是高速数据传输，因此攻击者可以主攻DIO接口，降低数据的输入和输出率，如增加COS(Change of State)中断等。当输入信号从高到低或从低到高变化，COS中断系统产生一个中断请求，使PCI控制器中断。每个输入通道都有COS中断的功能，默认情况下，COS中断功能是关闭的，管理者根据日期输入状态，需要打开一些特定通道中断功能。如果攻击者使更多的COS中断，系统经常中断，将大大减少数据输入速率，影响系统的功能；如果所有输入通道的COS中断被启用，它会导致拒绝服务，甚至系统瘫痪。

(5) 以太网接口测试：以太网接口的主要安全问题是缓冲区溢出和拒绝服务。

6.3 应用软件安全性测试

在信息系统中，作为整体，不仅要对硬件系统、网络系统进行测试，还需要对软件系统进行测试。由于系统的开发任务很大程度上是软件开发，因此测试的对象除了硬件部分、网络部分以外，更主要的是软件。

软件测试是使用为发现错误所选择的输入和状态的组合而执行代码的过程，它是在软件投入运行前，对软件需求分析、设计规格说明和编码的最终复审，在规定条件下对程序进行操作，以发现错误，对软件质量进行评估。它是根据软件开发各阶段的规格说明和程序的内部结构精心设计一批测试用例，用这些测试用例去执行程序，从而发现程序中错误的过程。软件测试的目的是通过系统的测试方法，发现软件中的错误，提供丰富的错误诊断信息，便于改正错误，预防错误的发生，减少软件开发的费用。

根据测试过程是否需要运行被测试的程序，软件测试方法一般分为静态测试方法与动态测试方法。

1) 静态测试

静态测试在对软件代码进行分析、检查和测试时不实际运行被测试的程序。静态测试方法还适用于对各种软件文档进行测试。

2) 动态测试

动态测试通过运行软件来检验软件的动态行为和运行结果的正确性。动态测试的主要特征是计算机必须实际运行被测试的程序，通过输入测试数据，对其运行情况进行分析。运行情况是指输入与输出之间的对应关系。

从是否针对系统的内部结构和具体实现算法的角度，软件测试方法可分为黑盒测试和白盒测试。

1）黑盒测试（功能测试）

黑盒测试，又称功能测试，它把被测试对象看成一个黑盒子，测试人员完全不考虑程序的内部结构和内部特性，只依据规格说明测试系统已定义的功能，检查程序的功能是否符合它的功能说明，检验程序是否与功能要求完全一致。黑盒测试的重点在于如何从输入域中选择待测的测试用例。由黑盒测试所产生的测试用例应能检验程序的全部功能。黑盒测试可以发现不正确或漏掉的功能、接口错误、数据结构或外部数据库访问中的错误、性能错误、初始化或终止错误等。黑盒测试的优点是能站在用户立场上进行测试，缺点是不能测试程序内部的特定位置，当规格说明有误的情况下也无法发现。

2）白盒测试（结构测试）

白盒测试，又称结构测试，它把被测试对象看成一个透明的白盒子，测试人员完全知道程序的内部结构和处理算法，按照程序内部结构和逻辑设计测试用例，对程序的路径和过程进行测试，检查是否满足设计的需要。白盒测试的测试用例用于检查模块中的独立路径，每个逻辑判定的真假，每个循环变量的初值、中间值和终值，程序的内部数据结构是否有效等。通过白盒测试可发现程序中的逻辑错误和不正确的假设或条件、未预料到的意外路径、语法检查未发现的书写错误等。白盒测试的优点是能够对程序内部的特定位置进行覆盖测试，缺点是无法检验程序的外部特性，无法对未实现规格说明的程序内部欠缺部分进行测试。

软件安全是软件领域的一个重要子领域，已经成为评判软件质量的一个重要标准。软件安全性作为软件质量的一个重要属性，表达了软件在系统工作中避免不可接受风险的能力以及软件运行不引起系统事故的能力，是保证系统安全、避免重大人员伤亡和财产损失的重要环节。安全性一般分为两个层次：应用程序级别和系统级别。应用程序级别包括对数据或业务功能的访问，确保在预期的安全性情况下，操作者只能访问特定的功能、用例或者有限的数据。系统级别包括对系统的登录或远程访问，确保只有具备系统访问权限的用户才能访问应用程序，而且只能通过相应的入口来访问。软件安全性包括失效安全性和保密安全性，传统上关注较多的是软件的失效安全性。失效安全性是软件运行不引起系统事故的能力，强调的是一类安全关键软件的安全性失效可能造成重大人员伤亡、财产损失和环境污染等危险事故。对失效安全性的度量主要有建立在可靠性理论基础上的安全度、失效度、平均事故间隔时间和软件事故率等。失效安全性测试常用的测试方法主要有基于故障树的测试和基于最小割集的测试。对于保密安全性，ISO 9126 质量模型的定义是“与防止对程序和数据进行非法存取的预防能力有关的质量属性”。保密安全性测试主要的测试方法有代码走读与审查、静态分析、形式化方法、故障注入、基于模型的测试、基于属性的测试、语法测试、模糊测试等。

在工程项目中，常规的软件工程方法和软件测评手段并不能完全验证软件安全性，需要通过软件安全性测试来验证与软件相关的系统危险已被消除或被控制在可接受的风险水平。通过测试可在软件中发现隐藏的重大错误并进行排除。但在工程中开展软件安全性测试仍然比较困难。

6.3.1 软件安全性测试方法

软件安全性测试是验证软件的安全等级和识别潜在安全性缺陷的过程，一般包括运行环境的可靠性和数据存储的安全性。软件安全性测试过程包括安全功能测试、渗透测试与验证过程。软件安全性测试不同于其他测试类型，安全性缺陷也不同于一般的软件缺陷。一个很难发现的软件缺陷可能只影响很少一部分用户，但一个很难发现的软件安全漏洞可能导致大量用户受到影响。安全性测试和传统测试最大的区别在于它强调软件不应该做什么，而不是软件要做什么。非安全性缺陷常常是违反规约，即软件应该做 M，它却做了 N。安全性缺陷则是软件应该做 M，它做了 M 的同时，又做了 N。传统测试类型强调软件的肯定需求，例如用户账户登录失败 5 次则关闭此账户，而安全性测试更强调软件的否定需求，例如未授权用户不能访问数据。

软件安全性测试可分为安全漏洞测试和安全功能测试。安全漏洞是指系统在设计、实现、操作和管理过程中存在的可被利用的缺陷或弱点。漏洞一旦被利用，可能造成软件受到攻击，软件就进入不安全的状态。安全漏洞测试是从攻击者的角度发现软件的安全漏洞的测试。安全功能测试基于软件的安全功能需求说明，测试软件的安全功能实现是否与安全需求一致，需求实现是否正确完备。软件安全功能需求主要包括数据机密性、完整性、可用性、访问控制、授权、身份认证、不可否认性、审计跟踪、委托、隐私保护和安全管理等。

1. 软件安全性测试的主要模型

随着对软件安全性的研究越来越多，安全性测试方法相关研究取得了一定进展。以下是软件安全性测试方法的主要模型。

1）形式化安全测试

形式化安全测试通过建立软件的数学模型，在形式规格说明语言的支持下，提供软件的形式规格说明。形式化安全测试可分为两类：模型检验和定理证明。模型检测用状态迁移系统 P 描述软件的行为，用时序逻辑、计算树逻辑或演算公式 Q 表示软件执行必须满足的性质，通过自动搜索 P 中不满足公式 Q 的状态来发现软件中的漏洞。定理证明将程序转换为逻辑公式，使用公理和规则证明程序是一个合法的定理。

2）静态安全性分析

静态安全性分析主要通过对源代码进行安全扫描，根据程序中数据流、控制流、语义等信息与其特有软件安全规则库进行匹配，从中找出代码中潜在的安全漏洞。静态安全性分析可以在编码阶段找出所有可能存在安全风险的代码，使得开发人员可在早期解决潜在的安全问题。

3）基于故障注入的安全性测试

基于故障注入技术的安全性测试建立应用与环境交互的故障模型。故障注入主要针对应用与环境的交互点，包括用户输入、文件系统、网络接口和环境变量等引起的故障。故障注入可以有效地模拟各种异常程序行为，通过故障注入函数强制使程序达到采用常规的标准测试技术无法达到的某些特定状态。

4）基于模型的安全性测试

基于模型的安全性测试对软件的行为和结构进行建模，生成测试模型，根据测试模型生成测试用例以驱动软件测试。测试用例的选择问题可以看作是从庞大的输入或状态组合

中，搜寻那些可以发现错误的状态及组合。如果不使用抽象的手段，有效的测试是不可能达到的。常用的软件安全性测试模型有 UML 模型、有限状态机和马尔可夫链等。

5）基于属性的安全性测试

基于属性的安全性测试采用 TASPEC 语言对软件的安全属性进行描述，首先确定安全编程规则，然后将规则编码作为安全属性，验证程序代码是否遵守了安全规则。基于属性的安全性测试针对目标软件的特定安全属性进行测试，可满足安全属性的优先级排序和分类要求，且部分与具体软件无关的属性说明是可重用的。

6）语法测试

语法测试的主要思想是根据被测软件的功能接口的语法生成测试输入，检测被测软件对各类输入的响应，软件的接口明确或隐含地规定了输入的语法。接口包括多种类型：文件、命令行、环境变量和套接字等。语法测试的步骤是识别被测软件接口的语言后，采用 BNF 或正则表达式定义语言的语法，语法定义了软件接受的输入数据的类型和格式。根据语法生成测试用例，然后进行测试。生成的测试输入应包含各类语法错误、符合语法输入的和不符合语法的输入等。根据被测软件对各类输入的处理情况，确定被测软件是否存在安全缺陷。语法测试适用于被测软件有较明确的接口语法且语法易于表达并生成测试输入的情况。语法测试结合故障注入技术可使得测试效果更好。

7）模糊测试

模糊测试将不合逻辑的随机数据插入程序，检查程序是否能容忍杂乱输入，以发现安全漏洞或采用其他逻辑思维难以发现的安全缺陷。模糊测试只是产生杂乱数据攻击程序，并不符合逻辑。模糊测试可使用语法规则来产生正常的输入，也可用基于特定程序的输入结合试探法来指导输入变量的生成。

8）基于渗透的安全性测试

渗透测试使用人工方法或者自动化工具模拟黑客输入，对应用系统进行攻击性测试，从而找出软件运行时存在的安全漏洞。渗透测试根据是否采用直接进入目标系统或网络内部的方式去收集信息，一般可分为主动攻击和被动攻击两种类型。渗透测试的结果一般都比较真实有效，发现的问题都是正确且比较严重的，缺点是模拟的测试数据只能到达有限的测试点，覆盖率很低。

9）基于风险的安全性测试

基于风险的安全性测试将软件开发过程结合风险分析与管理和安全测试，在软件开发各个阶段将有风险的安全漏洞考虑在内，通过风险分析、误用模式、异常场景和渗透测试等技术，尽可能早地发现高风险的安全漏洞。基于风险的安全性测试的实质是将安全测试相关过程集成到软件开发生命周期中去，在最短的时间内以最少的资源有效地达成用户需求，确保软件质量，减轻后期的维护工作。

2. 典型的软件安全性测试方法

根据特点的不同，可将软件安全性测试方法分为 3 类：基于形式化模型的软件安全性测试方法、基于可靠性分析方法的软件安全性测试方法和基于软件测试方法的软件安全性测试方法。下面对这些方法进行详细描述，并进行分析比较。

1）基于形式化模型的软件安全性测试方法

根据前面的介绍我们已经知道，形式化软件安全性测试方法可分为两类：模型检验方

法和定理证明方法。

(1) 基于模型检验的软件安全性测试方法。

模型检验方法用状态迁移系统 P 描述软件的行为,用逻辑公式 Q 表示软件执行必须满足的性质,通过自动搜索 P 中不满足公式 Q 的状态来发现软件中的漏洞。

模型检验技术的基本思想是用自动机模型表示系统,用某种逻辑公式来表示系统要验证的属性,采用穷举状态空间的方式来证明系统的模型是否满足要验证的属性。此方法利用内置的结构形式分析,即模型检验中的状态机描述来驱动测试过程,给测试工程师提供了生成和评估安全性测试集的方法。

模型检验方法的流程如图 6.3 所示。其中,方框代表测试过程中的活动。在此图中,系统规格说明和覆盖率标准共同驱动测试需求,测试需求通过检验模型再次评估系统需求,每个模型检验的范例对应一个满足给定测试需求的测试用例,通过收集和裁剪这些用例消除各种冗余,最后生成满足所有可行测试需求的测试集。测试集的测试需求符合与系统规格说明相关的覆盖率标准。

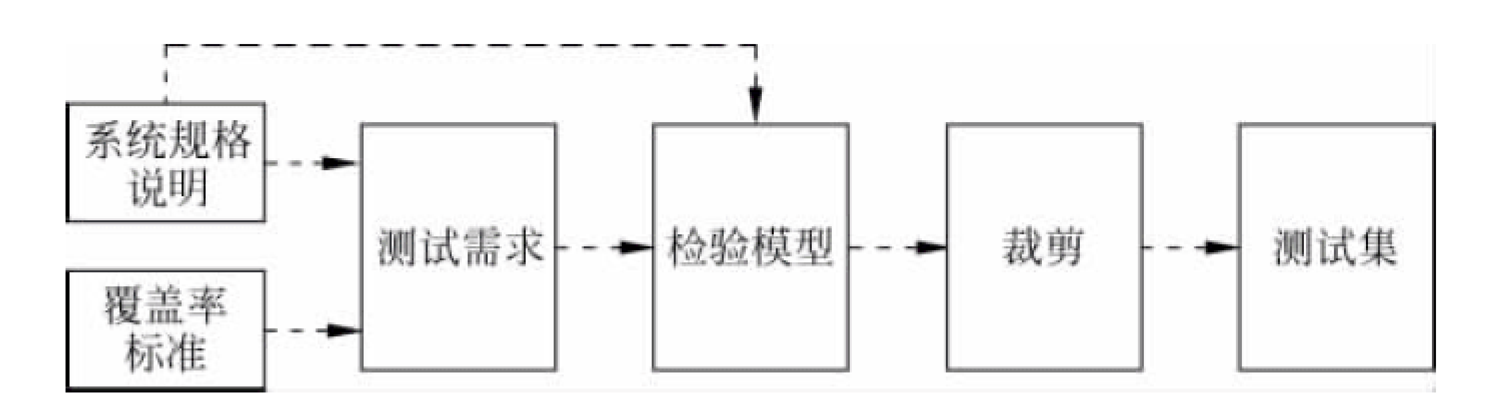


图 6.3 模型检验方法生成测试集

(2) 基于定理证明的软件安全性测试方法。

基于定理证明的软件安全性测试方法将程序转换为逻辑公式,然后使用公理和规则证明程序是一个合法的定理。基于定理证明的软件安全性测试方法一般只用于验证设计阶段的程序规范而非实际代码,原因是定理证明过程非常耗时费力。

2) 基于可靠性分析法的软件安全性测试方法

(1) 基于故障树分析的软件安全性测试方法。

基于故障树分析的安全性测试利用故障分析树和故障树的最小割集生成软件安全性测试用例。故障树分析法将系统故障形成的原因由总体到部分按树状划分,以系统最不希望发生的事件作为故障树的顶事件,寻找导致这一故障发生的全部可能因素,用倒立树状图形表示出顶事件与底事件之间的逻辑关系,绘制故障树,然后搜索出最小割集,并以最小割集为依据生成软件安全性测试用例。最小割集是由故障树的某几个底事件组成的集合,该集合中的底事件同时发生能引起顶事件的发生,并且去掉此集合中任何一个底事件将不再能引起顶事件的发生。对大型复杂软件系统的测试使用基于故障树的安全性测试,能够有效提高测试效率,明显提高测试的自动化程度和软件安全性测试的充分性。

故障树中底事件的语义解释根据应用领域的不同而不同,因此出现了一种基于形式化故障树分析建模的软件安全性测试方法。它将故障树的叶节点语义形式化为一个实时间隔逻辑持续时间计算公式,此公式以时间为变量,消除故障树的语义模糊性,形成形式化故障树。基于形式化故障树分析的安全性测试方法对软件需求规格说明进行等级划分,利用形式化故障树表示安全性需求,搜索出形式化故障树的所有最小割集,在此基础上运用基于割

集的安全性测试用例动态扩展算法来设计测试用例。

(2) 基于Petri网的软件安全性测试方法。

Petri网具有简洁、直观和潜在模拟能力强等特点,基于Petri网的软件安全性测试方法利用这些特点,在因果关系作用下进行推演,体现了系统的动态行为特征。基于Petri网的软件安全性测试方法有两种:正向分析法和逆向分析法。

正向分析法的过程是首先建立完整的状态标识表和可达图,得到Petri网的可达集,建立相应的Petri网模型,然后在可达集中搜索包含任意一个状态的所有状态标识,并将这些标记为危险标识,从初始状态到该危险标识的每个变迁序列均可设计为一个测试用例。每个危险标识应至少生成一个用例,这些用例构成了针对该Petri网模型的软件安全性测试用例集。正向分析法可以快速地求出测试用例集,并能有效地提高测试自动化程度。

对于逻辑和结构比较复杂的系统,正向分析法生成完整的可达图和状态标识集是比较困难的,而且容易形成组合爆炸的问题,这是正向分析法的缺陷。而逆向分析法构造所有可能导致软件危险的危险状态,然后分析求出由初始状态到该危险状态可能的路径,通过构造测试用例来验证该路径是可行的。逆向分析法要针对具体问题具体分析。

3) 基于软件测试方法的软件安全性测试方法

(1) 基于接口语法的软件安全性测试方法。

语法测试的主要思想是根据被测软件的功能接口的语法生成测试输入,检测被测软件对各类输入的响应,软件的接口明确或隐含地规定了输入的语法。软件的接口包括多种类型:数据总线、文件、命令行、环境变量和套接字等。接口语法测试定义了软件所接受的输入数据类型和格式。

基于接口语法的软件安全性测试的步骤如下:

① 识别被测软件接口的语言,定义语言的语法。

② 根据语法生成测试用例。其中,生成的测试输入应包含各类语法错误、符合语法的输入和不符合语法的输入等。

③ 通过执行测试检验被测软件对各类输入的处理情况,确定被测软件是否存在安全缺陷。

接口语法测试法适用于被测软件有较明确的接口语法且语法易于表达并生成测试输入的情况。语法测试结合故障注入技术可以得到更好的测试效果。

(2) 基于猜错法的软件安全性测试方法。

基于猜错法的软件安全性测试方法依据经验、直觉或对被测试系统的兴趣,在按规则生成的测试用例集之外添加一些另类的用例。此方法可为用例所涉及的实体定义一系列关系,借助这些关系实现用例的自描述,并和新的软件测试背景匹配,实现用例的再生。用例的自描述和再生过程也需要一系列的规则,这些规则是基于用例描述的,而非基于功能需求的。规则只存在于被描述的用例中,随着猜错用例描述的不同而不同。用例之间在描述上都是相互独立的,在运算上也不会相互牵制。由于猜错用例的总数是有限的,将其纳入测试自动化后,要将测试任务运算量上的增加限制在可接受的范围内。

利用这种方法可以解决用例的测试自动化问题,还可以提高测试的充分性。

下面对上述各种软件安全性测试方法进行分析对比:

(1) 基于形式化模型的软件安全性测试方法。

① 基于模型检验的软件安全性测试方法优点是可以生成满足所有可行测试需求的测试集，去除了人工参与，减少了出错的可能性，与传统测试方式相比，采用了穷举方式，更能保证软件的质量。缺点是测试准则和检验模型不易建立，而且减少冗余测试用例的算法实现起来比较困难。由于需要穷尽程序的所有实际执行状态，导致模型检验的效率较低，对于无穷状态系统更加难以检验。

② 基于定理证明的软件安全性测试方法的证明过程非常耗时费力，一般只用于验证设计阶段的程序规范而非实际代码，导致实际使用范围受到了一定的限制，而且定理证明过程难以完全自动化，需要高素质分析人员的大量参与。

(2) 基于可靠性分析方法的软件安全性测试方法。

① 基于故障树分析的软件安全性测试方法利用了故障树的最小割集，提高了软件安全性测试的充分性，而且便于推广，缺点是故障树分析和最小割集搜索过程的工作量较大，而且从安全性需求到形式化故障树的转化不易实现。使用该方法时需要通过自动化手段来减少人工的工作量，同时要明确从安全性需求到形式化故障树转化的方法和准则。

② 基于 Petri 网的软件安全性测试方法分为正向分析法和逆向分析法。正向分析法利用了 Petri 网的特点，有助于进行全面分析，缺点是需要生成完整的状态标识集和可达图，对逻辑和结构复杂的系统的分析较难完成，而且容易形成组合爆炸的问题。逆向分析法虽然可以避免组合爆炸问题，但是这种分析并不全面，需要针对具体问题进行具体分析，而且由初始状态到危险状态的路径分析很难通过人工实现，因此逆向分析法常用于分析系统关键层或模块。

(3) 基于软件测试方法的软件安全性测试方法。

① 基于接口语法的软件安全性测试方法的优点是可以与软件测试过程结合，节约测试成本，易于表达语法和生成测试输入，缺点是使用范围有限，需要与其他方法配合使用进行测试。接口的不同也增大了方法推广的难度。

② 基于猜错法的软件安全性测试方法经过自描述处理后生成测试用例，这些用例具有普遍适用性，自描述用例可以根据在新的软件测试任务中找到匹配的背景，重新变成在新背景下的测试用例。缺点是用例自描述和再生过程规则不易实现，而且用例生成方法主观因素较大，对分析者的要求较高，不易推广使用。

通过对上述软件安全性测试方法进行的分析对比，它们的优缺点如表 6.1 所示。

表 6.1 各种软件安全性测试方法的分析对比

<table>
<tr><th colspan="2">软件安全性测试方法</th><th>优 点</th><th>缺 点</th></tr>
<tr><td rowspan="2">基于形式化模型的软件安全性测试方法</td><td>基于模型检验的软件安全性测试方法</td><td>1. 去除了人工参与，减少了出错的可能性
2. 采用穷举方式，更能保证软件的质量</td><td>1. 测试准则和检验模型不易建立
2. 减少冗余测试用例的算法实现比较困难
3. 模型检验的效率较低，很难检验无穷状态系统</td></tr>
<tr><td>基于定理证明的软件安全性测试方法</td><td>1. 通用性强
2. 逻辑性较为严密</td><td>1. 定理证明过程难以完全自动化
2. 证明过程耗时费力，实际使用范围受到了一定的限制</td></tr>
</table>

续表

<table>
<tr><th colspan="3">软件安全性测试方法</th><th>优　点</th><th>缺　点</th></tr>
<tr><td rowspan="3">基于可靠性分析法的软件安全性测试方法</td><td colspan="2">基于 FTA 的软件安全性测试方法</td><td>1. 有利于满足软件安全性测试的充分性
2. 便于推广使用</td><td>1. 故障树分析和最小割集搜索过程的工作量较大
2. 从安全性需求到形式化故障树的转化不易实现</td></tr>
<tr><td rowspan="2">基于 Petri 网的软件安全性测试方法</td><td>正向分析法</td><td>1. 简洁、直观、潜在模拟能力强
2. 有助于进行全面分析</td><td>1. 对逻辑和结构复杂的系统的分析较难完成
2. 容易形成组合爆炸</td></tr>
<tr><td>逆向分析法</td><td>1. 可以对常用危险进行分析，缩小分析范围
2. 避免组合爆炸问题</td><td>1. 分析不全面
2. 由初始状态到危险状态的路径分析通过人工很难实现</td></tr>
<tr><td rowspan="2">基于软件测试方法的软件安全性测试方法</td><td colspan="2">基于接口语法的软件安全性测试方法</td><td>1. 可以节约测试成本
2. 易于表达语法并生成测试输入</td><td>1. 使用范围有限
2. 不易推广使用</td></tr>
<tr><td colspan="2">基于猜错法的软件安全性测试方法</td><td>1. 生成的用例具有普遍的适用性
2. 可以提高软件安全性测试的充分性</td><td>1. 用例自描述和再生过程的规则不易实现
2. 用例生成方法主观因素较大，不易推广使用</td></tr>
</table>

通过表 6.1 可以看出，以上这些软件安全性测试方法各有优缺点，在使用这些方法时需要综合考虑各方面因素，制定合理的测试策略。例如，在测试时可以先通过基于可靠性分析方法对测试的全面性进行把握，然后运用定理证明法验证设计阶段的程序规范，使用模型检验法提高测试效率，最后可用猜错法或接口语法测试进行补充。

6.3.2　软件安全性测试过程

软件安全性测试包含的内容如下：

(1) 验证每个软件安全性需求都有相应的软件安全性测试相对应。

(2) 证明每个软件安全性需求都通过一个或多个测试得到了满足。

(3) 通过测试分析和软件实现，评估相关的风险。

(4) 判断给出的软件安全性测试具有充分性。

软件安全性测试的主要过程如图 6.4 所示。

(1) 确认软件安全性测试规程。

要求软件安全工程师检查所建立的规程，并验证规程是否完全地对软件安全性需求进行测试。

(2) 执行和监督软件安全性测试。

为了确认软件安全性测试规程和判断该规程对软件安全性可能产生的影响，软件安全性测试团队需要对软件安全性测试进行监督。

(3) 整理和分析测试数据。

要将测试数据整理为有用的形式，以便发现通常难以发现的异常数据。数据整理的过程是实现是通过抽取测试期间记录的数据来推导性能和其他参数，并将其表示为易理解的显示信息。

为了标识与安全性相关的异常和不安全的因素需要对测试数据进行分析。不安全因素

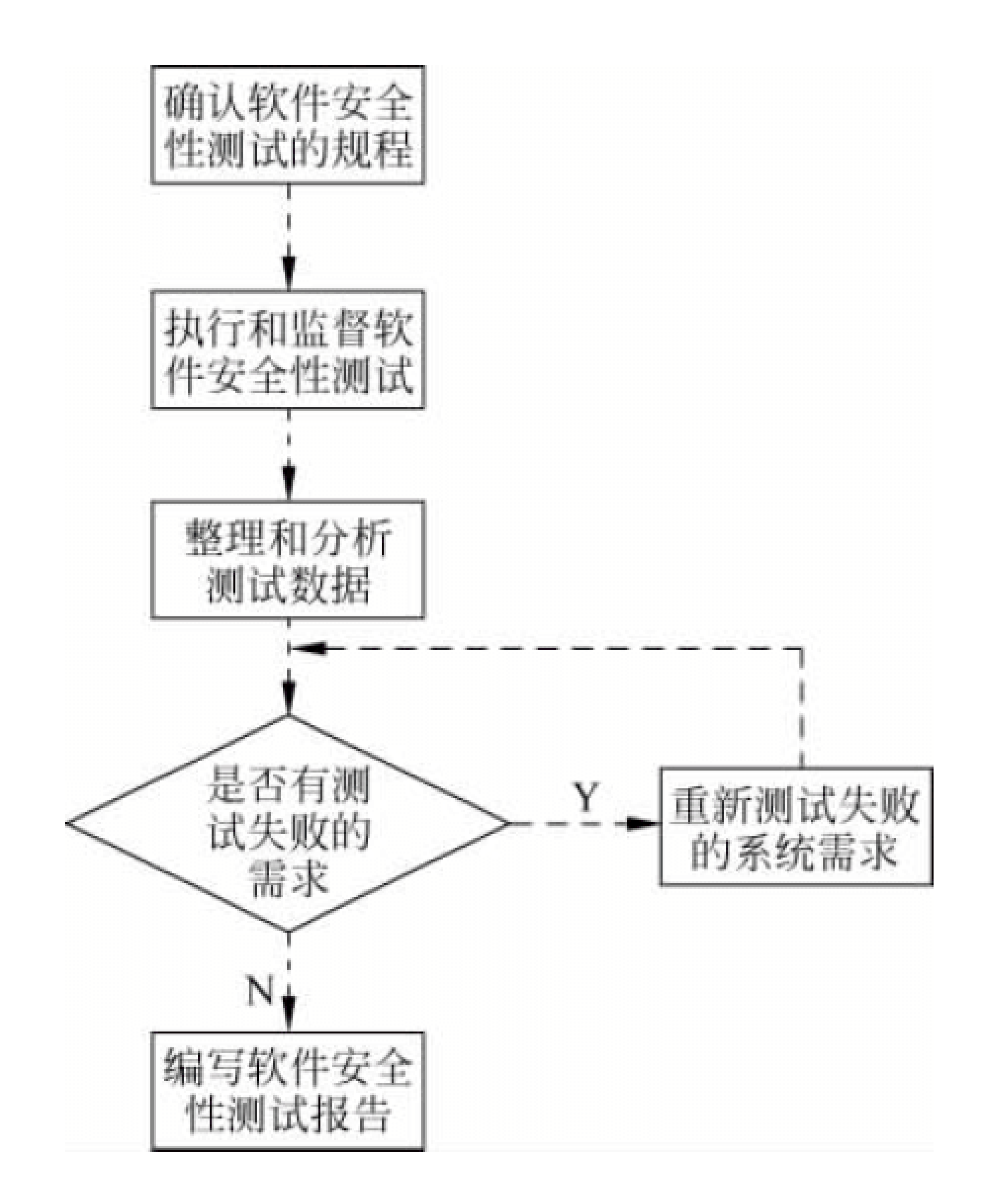


图 6.4 软件安全性测试过程

可能是规程、设计、实现、测试用例或测试环境中的错误。

(4) 重新测试失败的系统需求。

通常情况下，由于某些条件的限制，一次测试并不能确认全部的软件安全性需求，需要通过回归测试来保证功能的充分安全。

(5) 编写软件安全性测试报告。

软件安全性测试报告内容包括标识所进行的测试和分析测试的结果。在测试报告中，软件安全性测试团队使用测试结果来更新安全需求标准分析中的需求可追踪性矩阵，对系统和软件进行的初步分析和详细分析也需要进行更新。软件安全性测试报告附加到系统安全性测试报告中。

6.3.3 软件安全性测试工具

通过自动化或半自动化的方式，软件安全性测试工具可以验证系统安全功能是否正确运行，安全机制是否有效，并发现潜在的安全漏洞，这样可有效提高测试效率，降低软件的安全风险。

安全性测试工具有很多种。根据测试对象的层次可分为主机安全测试工具、网络安全测试工具和应用安全测试工具。这种分类方法跨度较大，范围设计较广，而且难以识别每类工具的功能、特点和属性，不利于测试人员选择。根据安全测试工具的不同功能，可将安全测试工具分为源代码分析器、数据库脆弱性扫描器、网络漏洞扫描器、Web 应用漏洞扫描器、Web 服务扫描器、动态分析工具、配置分析工具、需求验证工具、设计模型验证工具。

源代码分析器又可分为静态源代码分析器和高级源代码分析器。静态源代码分析器主要扫描源代码匹配安全缺陷代码模式，可检测格式化字符串、缓冲区溢出和竞争条件等安全漏洞。高级源代码分析器对代码执行数据流和控制流分析，以降低误报率，并根据安全漏洞类型或优先级生成问题报告。另外可以采用反汇编技术与模式识别技术，脱离源代码，扫描可执行二进制代码或 DLL 文件发现安全漏洞，执行更低层次的安全性测试，但是误报率较

高。对于 Java 字节码也可以进行扫描，以发现可能的安全漏洞。

数据库脆弱性扫描器以客户端形式执行各种 SQL 查询，查找数据库安全配置的相关弱点，如访问控制、授权和弱口令等。数据库脆弱性扫描器有渗透攻击和审计两种典型工作模式。数据库脆弱性扫描器易于使用，容易发现配置管理方面的安全漏洞，但对数据库中敏感数据缺乏语义理解。

网络漏洞扫描器的工作原理是远程扫描目标主机开放的端口、操作系统类型和运行的服务等，发现其相关的安全漏洞。

Web 应用漏洞扫描器模拟 Web 客户端，执行特权 URL 扫描，脆弱 CGI 扫描等。它记录 HTTP 交互，在后续交互中注入恶意负载，以观察响应数据，发现 SQL 注入、Cookie 中毒、跨站脚本和目录遍历等安全漏洞。

Web 服务扫描器主要用于测试 Web 服务的安全功能并识别安全漏洞。它可扫描 WSDL 文件，列举 Web 服务提供的方法，操纵方法调用生成的各种输入参数，测试 XML 消息加密、签名和签名验证等安全功能。

配置分析工具对主机、应用服务器和应用程序等的配置文件进行静态分析，发现与配置相关的安全问题。

动态分析工具在程序运行时构造异常场景，测试软件是否存在安全缺陷。它的功能包括记录函数执行信息，执行边界检查，截获系统调用，执行文件系统、网络接口、系统资源等故障注入，识别内存泄漏、类型不匹配和不可达代码等安全问题。

需求验证工具主要验证软件安全需求说明是否满足正确性、完备性和一致性。

设计模型验证工具验证软件的设计模型是否存在安全缺陷。

表 6.2 列出了一些常用的安全性测试工具。

表 6.2 常用安全性测试工具

工具类型	开源或免费	商用
源代码分析器	RATS，UNO，lawFinder，BOON，ASTREE，CQual，C Code Analyzer (CCA)，Jlint，ITS4，Splint，LAPSE，Csur，PHP-Sat，PMD；FxCop，BugScam；FindBugs	Source Code Analysis Suite，Prexis，K7，CodeAssure，Prevent，DevPartner SecurityChecker，C++ Test/JTest/TEST WebKing，CodeScan，CodeCenter，CodeSonar，DevInspect，SoftCheck Inspector，PolySpace；AspectCheck，BEAST；BugScan
数据库脆弱性扫描器	MetaCortex	AppDetective，Database Scanner
网络漏洞扫描器	SuperScan，NMAP，Nessus，Metasploit Framework	Internet Security Scanner，Retina，SARA，NTOSpider，GFI LANguard，SAINT
Web 应用漏洞扫描器	Nikto，Wikto，EOR，OWASP WebScarab，OWASP Berretta，Paros ProxySpike Proxy，Pantera	AppScan，Burp suite，WebInspect，N-Stalker Web Application Security Scanner，Acunetix Web Vulnerability Scanner
Web 服务扫描器	Pushtotest TestMaker，Foundstone WSDigger	SOATest，SOAPbox，SOAPSonar，SOAPScope，XRay Diagnosis，QEngine，WebServiceTester，e-TEST suite for Web Services Testing，LISA Complete SOA Test Suite
配置分析工具	Foundstone SSLDigger，PermCalc	Desaware CAS
动态分析工具	NProf，CLR Profiler	Compuware BoundsChecker

6.4 本章小结

本章介绍了信息系统安全测试方面的内容，简单地介绍了关于测试的基本概念和硬件安全方面的内容，详细地介绍了软件安全性测试的内容，主要介绍了软件安全性测试的几种方法，另外还对软件安全性测试流程和一些测试工具也进行了简单的介绍。

6.5 习　题

1. 信息系统测试的目标和原则是什么?
2. 概述硬件安全方面的内容。
3. 概述软件安全性测试的主要方法。
4. 简述常用的3类软件安全性测试方法，并进行比较。
5. 简述软件安全性测试的过程。
6. 简要列举一些软件安全性测试工具并说明其功能。

第 7 章　信息系统运营中的安全管理

安全管理在信息系统运营中占据重要地位。管理是在群体活动中为了完成一项任务，实现既定目标，针对特定对象，遵循确定原则，按照规定程序，运用适当的方法，所进行的计划、组织、指挥、协调和控制等活动。保障信息系统安全可靠并妥善管理信息资源是信息系统运营中的安全管理所要实现的目标。安全管理是信息系统安全体系结构中最具能动性的部分。实际上，很多安全事件和安全隐患的发生，与其说是技术上的不足，不如说是管理不善。随着信息技术的飞速发展，在运用高新技术安全产品的同时，安全管理仍然是值得关注、不容忽视的。

7.1　安全组织结构

安全管理的实现依赖于组织的行为，信息系统的建设离不开各级机构的协调工作，做好安全管理工作必须建立与信息系统规模和重要程度相适应的安全组织结构。完善的安全组织结构是组织安全管理的前提条件。为了实现安全管理，组织应该设立专门的安全管理机构，并分配专门的安全管理人员，同时还应该建立完善的安全技术设施和安全管理制度。

1. 组织结构建设

信息系统运行效率的高低很大程度上取决于组织管理是否有效。为了有效实施信息系统安全方针，完成具体的安全活动并保护信息资产，组织应该确立信息安全组织机构并明确安全责任，明确与信息系统安全活动有关的管理、执行、验证等人员的职责，并确保职责的正确履行。组织应设立信息系统安全管理职能部门，领导管理信息系统的安全运营工作。部门成员包括安全管理主管、安全管理员、系统管理员、数据管理员、应用管理员、安全保密员、安全监督员、系统维护员以及数据备份专员等。加强各岗位人员之间、组织内部机构之间的合作与交流沟通，定期或不定期召开协调会议，共同协作处理信息系统安全问题。安全管理职能机构的成员及职责分配如下：

- 安全管理主管。负责组织、指导信息系统安全运行策略和方案，协调各方面人员完成系统信息处理任务，保证系统结构的完整性，确定系统改善或扩充的方向，并组织系统修改及扩充工作。
- 安全管理员。负责保障信息系统包括物理层、网络层、系统层、数据层、应用层在内的各个层面的安全管理，目标是整个系统安全、可靠地运行。
- 系统管理员。负责按照信息系统规定的制度与规程对系统环境、硬件设备、系统软件、网络情况进行日常的运行管理，保障系统的安全稳定运行。
- 应用管理员。对信息系统应用程序软件进行安装部署和管理，同时在安全管理主管的组织之下，完成系统的修改和扩充，保障信息系统的可用性。

- 数据管理员。负责数据库的管理以及数据层面的安全保障。定期对数据进行备份，当数据出现问题时按要求及时恢复，保障数据的完整性和有效性。
- 安全保密员。贯彻落实安全保密制度，执行信息系统安全保密工作，确保系统敏感信息在传输和存储过程中的机密性和完整性。
- 安全监督员。负责监督和检查系统安全运行的执行情况。
- 系统维护员。负责信息系统网络和设备的安装、维修、维护、升级、管理、使用和保养等工作。
- 数据备份专员。负责重要信息资源和关键设备的备份工作。

2. 组织安全管理

1）信息处理设施授权

信息处理设施包括计算机网络设施、硬件设备、通信设施、软件、安全产品等。对信息处理设施的采购、验收和授权过程应遵循严格的管理制度，设施的审批与验收能够防止产品质量问题和安全隐患，避免新设施无法兼容原有设施的情况出现。信息处理设施的使用应该经过严格的授权，防止非授权用户滥用。

2）审核和检查

根据组织制定的系统审核和检查规范，遵照程序定期执行系统审核和系统检查活动，并由专人负责检查包括网络环境、系统运行、漏洞及数据备份等情况。系统内部人员或上级单位负责定期进行系统全面检查，包括系统管理制度的执行情况、安全策略与安全配置是否一致、现有技术措施是否有效等。系统检查结果经过汇总，形成详细的系统检查报告。

3）信息系统安全独立审计

组织机构对信息系统安全方针的评审应保持相对的独立性，即被审核方与审核方应无直接利害关系，确保审计结果的公平与公正。审核方式包括内部审核与第三方审核两种。

4）信息安全专家建议

组织机构应指定具有一定安全技术和实践经验的内部技术人员作为组织内部的信息安全方面的顾问，负责在信息安全方面提供咨询建议。当信息安全事故或故障发生时，安全顾问能够提供技术支持。另外，安全顾问还会通过不同的渠道收集信息安全技术与管理上的安全措施，在组织内部进行沟通。为了紧跟行业趋势，了解最新评估方法和监督标准，组织应发展与外部安全专家之间的联系。由于外部专家能够带来专业知识和独立见解，许多组织都开始依靠外部安全专业人士，一些经常用到的专家有信息系统审计员、数据恢复分析师等。

5）第三方访问权限控制

企业外部的人员或组织，如业务合作伙伴、供应商或承包商等作为第三方要求对信息系统进行访问时，组织要按照严格的安全策略，控制第三方对信息和信息系统的访问类型。首先系统要对第三方访问执行风险评估，第三方访问的结果可能会产生敏感信息的泄露、资产损害等风险，组织应该根据风险评估结果制定控制措施并予以实施。组织应该明确规定第三方访问信息资源以及设备的权限和责任，尤其是对敏感信息和关键设备的访问，都要做出明文规定并详细记录在案。

7.2　安全人事管理

信息系统是由人研制开发的,目的是为人类服务的工具。影响信息系统安全的因素,除了少数难以预测的自然灾害以外,绝大多数的安全威胁都来自人类自己,如有意对信息系统进行攻击和破坏的黑客、计算机病毒,以及无意的操作失误等。因此,人始终是影响信息系统安全的最大因素,人事管理是安全管理重要组成部分。全面提高信息系统相关人员的技术水平、道德品质、政治觉悟和安全意识是信息系统安全最重要的保证。

1. 人事审查

内部人员所引发的安全事件不在少数,系统的安全堡垒往往容易从内部攻破,所以内部管理人员的素质十分重要。人事管理的核心是确保有关专业人员具备良好的专业素质、职业道德、思想素质和业务素质。人事审查是加强人员管理的第一关,要审查的内容包括人员的安全意识、法律意识、安全技能以及人员素质等方面。

1) 安全审查标准

政治可靠、作风正派、思想先进和技术合格等是信息安全管理人员应具备的基本素质。

不同安全等级的信息系统人事审查标准不同,人事审查必须根据信息系统所规定的安全等级确定审查标准。例如,对于管理机要信息的信息系统,必须按照审查机要人员的标准审查所有能接触到该系统的工作人员。

必须保证关键岗位人员的绝对安全可靠,并不得存在其他岗位人员兼职的情况。必须经过严格的政审,并要考核其业务能力才能确定信息系统管理关键岗位人选,包括系统管理员、安全负责人、安全管理员、安全设备操作员和保密员等。例如,对安全负责人的审查不仅要通过严格的政审,还要考虑工作表现及态度、道德修养和业务能力等方面。

人事审查首先要制定合理的人事安排方案,然后因岗选人。应遵循"先测评,后上岗,先试用,后聘用"的原则。组织安全管理机构要明确所有人员在信息系统安全管理中的责任和权限。在实际操作中要将人员的工作、活动范围限制在可以完成任务的最小范围内。对于可能涉及机密信息的人员,应当明确告知其所承担的保密义务和相关责任,要求做出保密承诺。

2) 人事安全审查

对于人事审查应当有详细的人事安全审查记录,并对其进行备案,不管是正在使用的人员还是新录用的人员和预备录用的人员。

人事安全审查主要是指审查对于可能接触到保密信息的人员其自身素质是否与其所承担的保密义务相适应,检查其是否值得信任。审查的内容主要包括人员的政治表现、保密意识、纪律性、学历真实性、简历的完整性、身份证明、业务熟练程度、价值观、是否诚实可靠、有无不良记录、身体状况等。

对于临时聘任或者接受中介推荐给组织的人员也要进行安全审查。尽量不要让临时聘任的人员接触保密级别较高的信息,对于可能接触到这些信息的临时工作人员更要进行详尽的审查。对于中介推荐的人员,组织要与中介签订合同,明确要求中介机构要对被推荐人进行审查,如有疑虑或怀疑,必须及时通知组织。对于中介机构推荐者,组织最好也要对其

展开独立的审查。

管理人员要对新来人员进行培训和监督，尤其要监督那些得到授权接触敏感系统的工作人员。另外，所有工作人员的工作都要进行定期审查。

2. 人员安全教育

人员带给系统的安全威胁通常来自两个方面：一是有关人员故意泄露；另一方面是信息安全管理人员安全意识淡薄，对信息安全管理的理解不到位，专业技能不足以担当所承担的保密责任。前一种安全威胁可以通过人事审查来防止信息泄露，后一种就需要通过安全教育，提高工作人员的安全意识，并确保其遵守组织的信息系统安全方针。

1）信息系统安全教育的对象

安全教育的对象，包括与信息安全相关的所有人员，主要有：

- 用户。
- 领导和系统管理人员。
- 信息系统的工程技术人员。
- 系统设备制造商。
- 法律相关人员。

2）信息系统安全教育的内容

安全教育和培训的内容要与培训对象所接触信息的保密等级相适应，主要包括法律法规教育、安全技术和安全意识教育。

（1）法律法规教育。

法律法规教育是信息系统安全教育的核心，与信息系统相关的所有人员（包括领导、管理人员和技术人员等）都应该接受信息系统安全的法律法规教育。

（2）安全技术教育。

信息系统安全管理的技术教育是组织信息系统安全的技术保证，常用的信息系统安全技术有加密技术、防火墙技术、防病毒技术、反垃圾邮件技术、漏洞扫描技术、入侵检测技术、备份技术等。为了防止相关人员使用信息系统时误操作引起安全威胁，应该对相关人员进行安全技术培训和教育。作为安全技术教育的一部分，还须了解信息系统的风险和脆弱点，以及与此有关的风险防范措施和技术。

（3）安全意识教育。

所有信息系统相关人员都应当接受安全意识教育，安全意识教育的主要内容包括：

- 组织信息安全方针与控制目标。
- 安全职责、安全程序及安全管理规章制度。
- 使用的法律法规。
- 防范恶意软件。
- 与安全有关的其他内容。

除了以上的教育和培训，组织管理者应根据相关人员所接触到的信息保密等级提供相适应的专业技能。

为确保与信息系统安全有关的所有人员均能得到必要的培训，并保证培训效果，分管培训的部门应对培训活动进行策划，编制培训计划并按计划要求实施培训，培训结束后还应通过适当的方式进行考核。

3. 人员安全保密管理

1）安全保密契约管理

组织要求员工工作之前签署一份包括不泄露组织秘密、道德准则和隐私问题在内的安全协定，明确员工的保密要求和责任。

进入信息系统工作的人员应签订保密合同，承诺其对系统应尽的安全保密义务，保证在岗工作期间和离岗之后一定时期内，均不得违反保密合同，泄露系统秘密。对违反保密合同的人员应进行惩处，对接触机密信息的人员应规定在离岗后的某段时间内不得离境。

保密协议的目的是对信息的保密性加以说明。雇员在受雇时，应和单位签署保密协议，并将此协议作为规章制度的一部分。没有签署保密协议的临时人员或第三方在接触信息处理设备之前必须签署临时保密协议。在雇佣合同或条款发生变动时，特别是员工要离开单位或其合同到期时，要对保密协议进行修订。

2）离岗人员安全管理

组织必须有人员调离的安全管理制度，例如，人员调离的同时马上收回钥匙、移交工作、更换口令、取消账号，并向被调离的工作人员申明其保密义务。

对于离开工作岗位的人员，要确定该工作人员是否从事过非常重要的信息方面的工作。任命或提升工作人员时，只要涉及接触信息处理系统，特别是处理敏感信息的系统，如处理财务信息或其他高度机密的信息系统，就需要对该员工进行信用调查。对握有大权的工作人员，此类信用调查更要定期展开。

（1）调离人员。

调离岗位人员应做到及时移交所有的系统材料，及时更换口令，重申离岗后承担的安全与保密责任和义务。

对调离人员，特别是在不情愿的情况下被调走的人员，必须认真办理手续。除人事手续外，还必须进行调离谈话，申明其调离后的保密义务，收回所有钥匙和证件，退还全部技术手册及有关材料。系统必须更换口令，取消其用过的所有账号。在调离决定通知本人的同时，必须立即或预先进行上述工作，不能拖延。

（2）解聘人员。

涉及信息系统安全管理的人员，在解聘时，应当进行严格的审查，并按照所签订的保密契约的规定来执行。

7.3　安全系统管理

要保证系统的可靠性、安全性和有效性，必须加强对系统运行的安全管理。运行中系统安全管理包括系统评价、系统运行安全检查和系统变更管理等。系统安全管理还应建立系统运行文档和管理制度。

1. 系统运行安全管理的目标

系统运行安全管理的目标是确保系统运行过程中的安全，主要包括可靠性、可用性、保密性、完整性、不可抵赖性和可控性几个方面。

1）可靠性

可靠性是系统能够在设定条件内完成规定功能的基本特征，是系统运行安全的基础。可靠性规定了系统功能所能满足任务性能要求的程度，也是系统有效性的体现。可靠性是系统安全审查的最基本的目标之一。

系统的可靠性分为两类，即软件可靠性与硬件可靠性。软件可靠性是指软件满足用户功能需求的性能和软件在规定环境下的故障率。硬件可靠性是指软件运行的系统整体环境的支持和性能度。提高系统可靠性，保证系统安全从原理上看就是要加强变化管理、提高规划质量、减少软件错误和提高系统容错能力。

2）可用性

可用性是系统可被授权访问实体访问并按任务需求使用的特性。可用性是系统面向用户的安全管理特性，是系统向用户提供服务的基本功能。系统的可用性具体是指系统无故障、不受外界影响、能稳定可靠地运行，能够随时满足授权实体或用户的需求，它包含了实体环境的稳定性、可靠性、抗毁性和抗干扰性等。系统的可用性必须保证系统的可恢复性，以保障系统遭受各种破坏之后能恢复系统运行环境，保持运行功能或在一定条件下允许系统降低运行功能。系统的可用性还应包括识别确认身份、访问控制、信息量控制和审计跟踪等要求。

3）保密性

保密性是系统信息不被泄露给非授权用户、实体或任务进程，或供其利用的特性。在系统中，应确保只有授权用户才能访问系统信息，必须防止信息的非法和非正常泄露。一般情况下，系统的保密性要对信息进行加密或隐藏保护，同时还要做到防入侵、防泄露、防篡改和防窃取。

4）完整性

完整性是系统在未经授权的情况下不能被改变的特性，是一种对系统可信性及一致性的度量。完整性是一种面向信息的安全性，它要求保持信息的原始性，即信息的正确生成、存储和传输。完整性的目的是要求信息不能受各种原因的破坏。系统完整性服务可以防范抵制主动攻击，使系统在信息传输、存储和交换过程中保证接收者收到的信息与发送者发送的信息完全一致，也就是确保信息的真实性。

5）不可抵赖性

不可抵赖性也称作不可否认性，是指在系统的信息交换中确认参与者的真实同一性，即所有参与者都不能否认或抵赖曾经完成的操作和任务。利用信息源监控证据可以防止访问用户对信息访问或操作进行否认。

6）可控性

系统可控性是通过计算机系统、密码技术和安全技术及完善的管理措施，保证系统信息资源在传输、交换和存储过程中完全实现安全审计目标。可控性是对系统的运行及有关内容具有控制能力的特性。可控性包括对系统信息访问主体的权限划分和更换，以及对信息交换双方已发生的操作进行确认，其中也包括对系统关键的控制。另外系统的可控性必须包含可审查性，即对系统内发生的与安全有关的事件均要有运行记录备查。

2. 系统评价

系统评价是对一个系统进行的质量检测分析，包括系统对用户和业务需求的相对满意

程度，系统开发过程是否规范，系统功能的先进性、可靠性和发展性，系统的性能、成本、效益综合比，系统运行结果的有效性、可行性和完整性，系统对计算机系统和信息资源的利用率，提供信息的精密程度和响应速度，系统的实用性和操作性，系统运行安全性及系统内数据信息的安全性等。

系统在投入运行以后，要不断地对其运行状况进行分析评估，并将结果作为系统维护、更新以及进一步开发的依据。系统评价指标如下：

1）预订的系统开发目标完成情况

- 对照系统目标和用户目标检查系统建成以后的实际情况。
- 系统是否满足科学管理和安全管理的要求。
- 用户的投入是否限制在规定范围内。
- 开发工程是否规范，各阶段文档是否齐备。
- 系统的维护性、扩展性和移植性如何。
- 系统内部各类资源的利用情况。
- 实现功能与投入成本比是否在用户规定的指标范围内。

2）系统运行实用性评价

- 系统运行的稳定性和可靠性。
- 系统的安全保密性能。
- 用户对系统操作、管理和运行状况的满意程度。
- 系统对误操作的保护和故障恢复能力。
- 系统功能的实用性和有效性。
- 系统运行结果对用户实际工作的支持程度。
- 系统运行结果的科学性和适用性分析。

3）系统对设备的影响

- 设备运行效率。
- 数据传输、输入、输出与设备处理的速度匹配情况。
- 各类设备的负荷情况以及利用率。

3. 系统运行安全检查

系统运行安全检查的目的主要是保证系统正常运行，使系统始终处于高效稳定的运行状态，获得最高的使用率和安全性。

计算机硬件系统实体及实体环境是一切系统运行的基础，没有这个基础，也就没有系统的应用，也就谈不上运行的安全管理。计算机硬件系统及实体环境安全检查的主要任务如下：

1）计算机硬件系统及实体环境检查

- 检查计算机主机设置及所用的备份设置是否正常。
- 检查工作人员进行批处理和系统日常维护的终端设备。
- 检查网络设备设置及网络状态。
- 检查进入机房的人员及系统操作员，并严格区分有关人员可以进入的区域。
- 检查机房环境，保证机房温度和湿度。
- 检查电源系统的可靠性，检查防火、防水警报系统的可靠性。

- 记录计算机硬件系统及实体环境状态检查情况,并形成日志报告。

2）系统运行安全测试

- 操作系统测试：确保系统安装运行所要求的指标以及设置参数正常有效。
- 系统安装测试：检查系统是否安装成功并达到运行指标要求。
- 系统单元测试：利用正常数据或非正常数据,测试系统每一个程序输入输出是否成功有效。
- 系统测试：对所有程序同时进行测试,以确保程序之间相互关系的正常有效。
- 容量测试：保证在系统所要求的常规条件下,能够处理系统设计所达到的最大数量。
- 综合测试：确保程序能够与其他的应用交互作用,并确保数据流正确有效,不会造成其他应用的问题。
- 目标测试：根据系统或应用中制定的执行目标及其他目标,检查系统是否完全满足用户需求。

4. 系统变更管理

信息系统和其他复杂系统一样,始终处于一种不断变化的状态。无论变化是出于内部因素还是外部因素,系统管理员都要花费大量的时间去调查、推断和排除对系统的影响。如何迅速解决由于信息系统不断变化而产生的问题,这就是变更管理涉及的内容。

1）运行同步跟踪

管理者持有信息系统各个方面的准确档案,将有助于排除故障,从而更有效地管理信息系统。为了维护信息系统安全运行,需要跟踪所有变化和升级,记录系统变化前后的状态。

(1) 标定基准线。

标记系统当前状态是正确维护信息系统的第一步。只有分析清楚系统当前以及过去的性能,才能预测系统将来的状态。测量和记录系统当前状态的操作称为标定基准线。基准线参数包括主干网的利用率、系统设备利用率、每日每小时登录的用户数、系统运行的协议数、错误的统计数等。

每个信息系统都要求标定它的基准线走势,测量的单元依赖于哪个对系统和用户要求最苛刻的功能。基准线参数允许将信息系统变化引起的性能变化和过去的系统状态进行比较,标定基准线是准确了解升级和改变是否有助于系统的唯一方法。如果预先绘制了信息系统区段利用率的趋势图,就可以帮助预测重大系统变化所产生的效果,例如,当系统需要升级时,它可以提供良好的分析和预测手段。

(2) 资产管理。

评估过程中另一个关键部分是检验和跟踪信息系统中的软硬件资产,这一过程被称为资产管理。资产管理的第一步是将信息系统中的每一个节点列出清单。系统软硬件的变化情况应该及时在资产管理数据库中进行自动或手动定期更新。另外,资产管理还应提供关于某些类型软件和硬件的花费和利益的信息。

(3) 变化管理。

对于信息系统管理和升级过程中的问题必须用管理系统进行跟踪。就像资产管理系统一样,变化管理系统要实时进行,另外还必须提供变化时间、变化的原因和对变化的具体描述。

2）软件修订

信息系统中软件的改变包括软件补充、软件升级和软件修订。尽管对每种类型的软件的改变不同，但是通常采用的步骤如下：

- 考虑改变（不论是补充、升级还是修订）是否必要。
- 研究改变的目的和对系统可能产生的影响。
- 考虑改变是适合于一部分用户还是所有用户，应该集中执行还是逐个执行。
- 如果打算实施改变，应告诉管理人员和用户，制定在非工作时间的改变进度。
- 在做任何改变之前都要备份当前的文件系统和软件。
- 防止用户登录正在被改动的系统或部分系统。
- 在安装、补充和修订时保持升级指导并按此进行。
- 实施改变。
- 在改变之后测试整个系统，留意任何修改的非预想和不满意的产物。
- 如果修改成功，就开放该系统的登录功能，如果没有成功，就恢复旧版本。
- 当修改成功后告知管理人员和用户。
- 如果必须恢复老版本，说明原因。
- 在变化管理系统中记录修改。

3）硬件和物理设备的变更

硬件和物理设备的改变是实现系统升级的一种重要手段。为信息系统增加功能，最简单、最重要的硬件改变是添加更多的设备，如在主干网上增加交换机或网络打印机等。在考虑硬件实施升级时，下面的步骤可以作为指导：

- 考虑变化是否需要。
- 研究变化对其他设备、功能和用户的潜在影响。
- 如果打算进行改变，就通知系统管理人员和用户，并安排在关机时间进行。
- 备份当前硬件设置。
- 阻止用户访问正在改变的系统。
- 实施改变。
- 在改变完成后彻底测试硬件。
- 如果安装成功，就打开系统登录功能，如果未成功，可能的话隔离该设备或重新插入旧设备。
- 当改变成功时通知系统管理人员和用户，如果不成功，解释原因。
- 在变更系统中记录修改。

5. 建立系统运行文档和管理制度

1）建立系统设置参数文件及运行日志

系统设置参数文件是记录备案系统运行时所设定的运行参数文件，包括系统启动文件、参数设置文件、检查记录、审计文件和口令文件等。系统设置参数文件记录备案是将系统初始状态、当前状态和各类程序运行参数设置进行安全备份，用于今后的系统运行维护、系统恢复和系统移植，也可用于对系统运行进行安全审查。

系统运行日志记录系统运行时产生的特定事件。运行日志是确认和追踪与系统的数据处理、任务进程及资源利用有关的事件的基础，它能提供系统权限检查中的问题、系统故障

的发生与恢复以及系统监测等信息,同时也用于检查系统的使用情况。运行日志的设置将减少系统运行错误和非法访问、窃取信息的机会。运行日志应记录哪些项目和记载的程度,要从系统的安全控制和用户需求这两方面来考虑。运行日志记录功能应该在系统设计时确定,一般情况下需要以下两种类型。

- 事件信息:包括数据的输入和输出、系统文件的更新和删除、系统的启动和关闭、系统故障的发生与排除以及用户的非正常操作等。
- 相关要素:如使用系统的人、设备、软件和数据等。

运行日志记载的信息是系统管理员对访问系统的人进行安全管理控制的重要根据,从安全管理角度考虑,此类信息在设计上必须要有法律依据,同时要求设计安全完善,不能因偶发事件或有意行为而破坏运行日志。

2) 建立科学的系统运行管理制度

为了保证系统安全运行,应建立科学的管理制度。管理制度包括各种岗位制度,如系统分析员的安全职责、系统管理员的安全职责及数据信息管理员的安全职责等;操作规范制度,如系统启动和关闭操作步骤及要求、注册登录操作步骤及要求等;系统维护及数据信息维护制度,如软件升级、病毒防治和数据备份等制度;另外还包括其他与系统安全运行相关的制度,如机房卫生、安全保卫制度,设备维护保养制度等。

7.4 安全事件管理

NIST在"Establishing a Computer Security Response Capability"一文中把安全事件定义为:任何威胁到数据的机密性、完整性或系统的完整性和可获得性的敌对行为。概括来说,安全事件就是指影响计算机系统和网络安全运行的一些不正当的行为。这些行为包括在计算机和网络上发生的可以观察到的任何现象,如对系统的破坏、非法获取或篡改数据等行为。对安全事件进行妥善的管理是信息系统安全的必然要求,具有很大的应用价值。

随着信息技术的迅速发展和信息系统的普及,信息系统安全管理逐渐成为一个重点。其中,安全事件管理是信息系统安全管理的一个重要分支。复杂的信息系统由种类繁多的安全设备、网络设备、主机系统及其应用等组成,每天产生大量安全事件,如何对之进行统一管理,通过对它们分析及时了解系统状况,发现潜在威胁和攻击,并在第一时间对异常事件做出快速响应,是信息系统管理亟待解决的问题,也是提高系统整体安全性能的关键。为了妥善解决以上问题,保障信息系统的正常运转,需要部署大量的安全设备。当攻击行为发生时,安全设备会在短时间内产生大量的安全告警事件,管理员很难在有限时间内从告警事件中获得有价值的信息。安全事件管理可以统一收集和管理这些安全事件,并将安全告警事件、网络设备和主机日志以及通过漏洞扫描获得的系统漏洞信息进行关联分析,能快速地发现网络攻击行为可能带来的危害,从而提高信息系统的安全性和可靠性。

安全事件管理作为一个新兴的面向应用、交叉性的研究领域,综合了入侵检测系统、防火墙等安全设备发来的事件,通过对其进行统一化、关联分析,从而做到对安全事故的自动识别和自动响应。安全事件管理具体的功能主要是安全事件的收集、分类、标准化、过滤、归并、关联分析和响应管理等。

7.4.1　安全事件生命周期

传统上，计算机和信息的安全注意力主要集中在保密性、完整性和可用性（即 CIA）上。过去发生的很多事件都很好地符合了 CIA 模型。事件大致可分为 6 类：垃圾邮件事件、入侵事件、DOS 事件、病毒和蠕虫事件、扫描事件和其他类型事件。对于垃圾邮件事件来说主要涉及可用性；对于入侵事件来说涉及 CIA 模型的 3 个方面；对于 DOS 事件来说涉及完整性和可用性；病毒和蠕虫事件也涉及 CIA 模型的 3 个方面；对于扫描事件则稍微涉及 CIA 模型的 3 个方面。

安全事件可以分为受理、启动、分析、处理、跟踪、关闭 6 个状态，各状态之间的关系如图 7.1 所示。

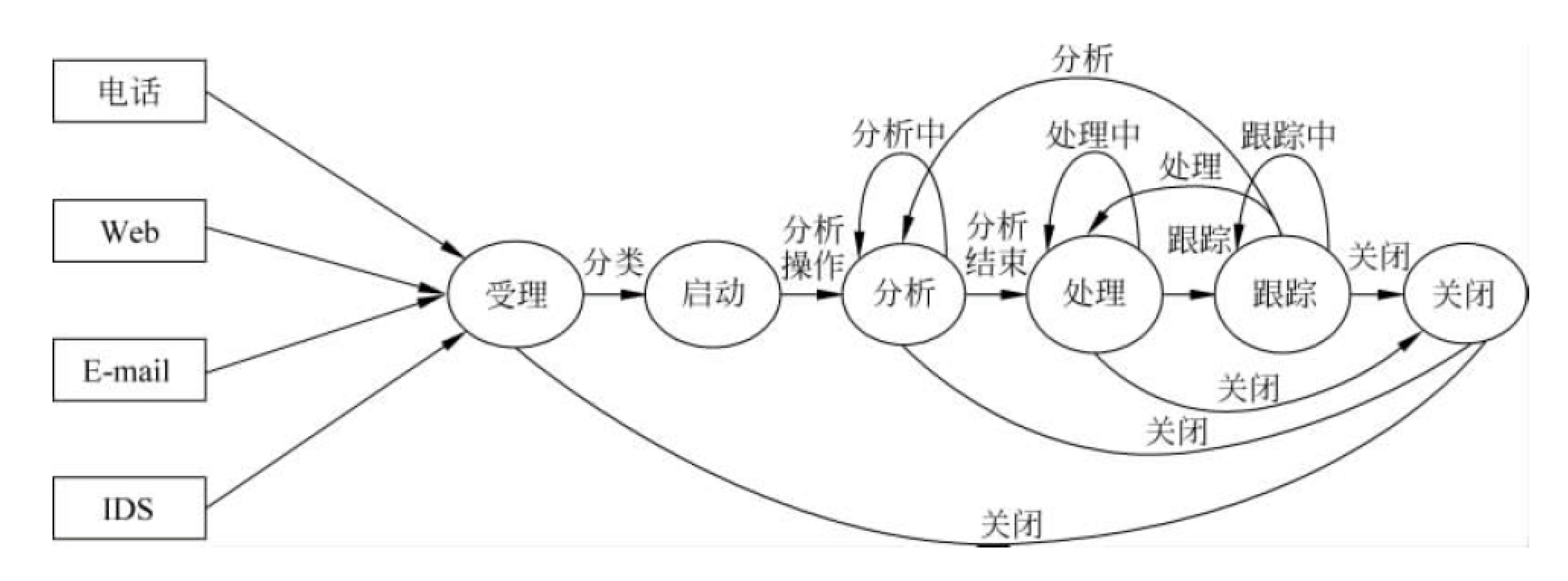


图 7.1　安全事件的状态及状态转换

系统的处理流程一般要经过事件报告、事件受理、事件启动、事件分析、事件处理、事件跟踪、事件关闭这几个过程。如图 7.1 所示，第一步收到来自电话、Web、电子邮件和监测系统的事件报告；第二步事件受理，并对事件进行分类、描述和判断其影响程度；第三步启动事件处理流程；第四步利用各种已有的工具对事件进行分析，得出分析结果；第五步事件处理，根据事件的性质和类型做出相应的处理；第六步对于需要跟踪的事件，建立一定的跟踪机制，对事件进一步观察；第七步关闭事件，关闭事件的条件有 3 个：

（1）投诉方认为事件已经结束不需要再进行处理。

（2）CCERT 小组成员认为事件已经圆满处理。

（3）超时，事件长期没有反馈信息，超时自动关闭。

安全事件响应过程从启动准备工作到事件后分析可以分为几个阶段。启动阶段包括建立和培训安全事件响应小组并获得必要的工具和资源。在准备工作中，组织也要以风险评估的结果为基础，通过选择和实施一套控制措施来限制安全事件的发生次数。但是即使在实施了安全控制措施后，残余风险依然不可避免，而且没有哪种控制措施是绝对安全的，所以对破坏系统安全的行为要进行检测，一旦安全事件发生要发出报警。针对安全事件的严重程度，采取必要的行动，通过对安全事件进行限制并最终从中恢复来减缓安全事件所造成的影响。在安全事件得到适当处理后，要提交一份报告，详细描述安全事件的起因、造成的损失以及以后对这类安全事件所应采取的防范措施和步骤。图 7.2 描述了安全事件响应的生命周期。

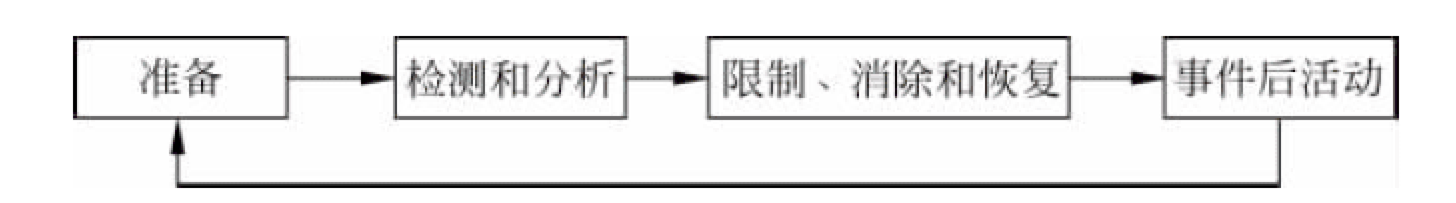


图 7.2 安全事件响应的生命周期

1. 准备阶段

安全事件响应方法通常都要强调准备工作，不仅要建立安全事件响应能力，使组织能够从容地响应安全事件，而且要通过确保系统、网络及应用足够安全来预防安全事件。下面将针对安全事件处理及预防的准备工作提供指导。

1）准备处理安全事件

安全事件处理过程中需要一些有价值的工具和资源的协助，对安全事件分析有用的资源包括：

（1）安全事件处理人员通信与设施。如安全事件响应小组的联系信息、安全事件报告机制、安全存储设施等。

（2）安全事件分析硬件和软件。如计算机取证工作站和备份资源、备用工作站、服务器及网络设备、数据包监听协议分析器、计算机取证软件、证据搜索辅助设备等。

（3）安全事件分析资源。如端口列表，包括常用端口和特洛伊木马端口。文档包括操作系统、应用、协议、入侵检测特征码、病毒特征码的文档。网络拓扑图和关键资产清单，比如 Web 服务器、邮件服务器、FTP 服务器。

（4）工具和资源。如预期网络、系统和应用的行为的基线。关键文件的加密哈希值，可以提高安全事件的分析、验证和消除速度。

（5）安全事件减缓工具。如介质，包括操作系统引导盘和 CD、操作系统介质及应用介质，还有安全补丁以及备份映像等。

2）预防安全事件

将安全事件发生次数保持在一个合理的数量之下是非常重要的。如果安全控制措施不充分，就可能发生大量安全事件，超出安全事件响应小组的能力，这将使安全事件响应迟缓和响应不完全，从而对组织造成更大的负面业务影响。一个改善组织的安全生态并预防安全事件的合理方法是定期对系统和应用进行风险评估。这些评估应该确定威胁和弱点所带来的风险，并将风险进行优先级排序。风险评估还可以用于确定关键资源，并进行重点监视和响应。

下面针对网络、系统和应用方面的安全管理策略进行简要介绍：

（1）补丁管理。

许多信息安全专家认为，大部分安全事件的发生是由于系统和应用中数量相对较少的弱点被利用所致。大型组织应该落实补丁管理项目来协助系统管理员确定、获得、测试并采用补丁程序。

（2）主机安全。

所有主机都应该被适当加固。除了保证为主机打上正确的补丁外，还应该对主机进行配置，只允许为适当的用户和主机开放尽可能少的服务，即最小特权原则。对于那些不安全的默认配置进行重置。当用户试图访问受保护资源时，要显示一个警告横幅。主机应该打

开审计功能,并记录与安全相关的重大事件。很多组织使用操作系统和应用配置指南来帮助管理员一致且有效地保护主机。

(3) 网络安全。

对网络边界进行配置,只有功能所必需的活动才被允许。这包括保护所有的连接点,比如调制解调器、VPN 及到其他组织的专线连接。

(4) 恶意代码预防。

应该在整个组织内采用能检测和阻止恶意代码(如病毒、蠕虫和特洛伊木马)的软件。应该在主机级(如服务器和工作站操作系统)、应用服务器级(如邮件服务器、Web 代理)和应用客户级(如邮件客户端和即时通信客户端)落实恶意代码保护。

(5) 用户意识和培训。

用户应该了解正常使用网络、系统和应用的政策和流程,从过去的安全事件中汲取经验教训,并与用户共享,从而提高用户的安全意识,减少安全事件发生的频率,尤其是恶意代码和违反安全政策的事件。对信息系统管理人员进行培训,严格按照安全标准维护网络、系统和应用。

2. 检测和分析

1) 安全事件分类

安全事件的发生方式多种多样,所以想要制定一个具体的综合流程来处理每一件安全事件是不切实际的。组织能做的最好程度就是从总体上准备处理任何类型的安全事件,对常见安全事件类型的处理则更具体一些。下面所列出的安全事件分类不是包罗一切的,也不打算为安全事件给出明确的分类,相反,它只给出了一个基本指南来指导如何根据其主要分类来处理安全事件。

(1) 拒绝服务攻击:通过消耗资源的方式来阻止和破坏网络与系统的正常使用。

(2) 恶意代码:能够感染主机的病毒、蠕虫、特洛伊木马或其他基于代码的恶意实体。

(3) 非授权访问:在未经系统允许的情况下通过逻辑的或物理的方式访问网络、系统、应用、数据或其他资源。

(4) 使用不当:用户违反可接受计算资源使用政策。

(5) 复合型安全事件:包含两种或两种以上的安全事件。

2) 事件征兆

安全事件响应过程中最困难的一步是准确检测并评估可能的安全事件,即确定一个安全事件是否会发生,如果发生,那它属于什么类型、影响程度如何以及问题的范围。安全事件的检测的影响因素包括:

- 安全事件的检测方法多种多样,不同的检测方法可以获得不同程度的细节和真实性。其中,自动化检测方法包括基于网络的和基于主机的入侵检测系统、反病毒软件以及日志分析工具等。另外,也可以通过人工方法来检测安全事件,比如用户报告的问题。有些安全事件有隐含的征兆,很容易被检测到,而有些安全事件,如果没有自动工具几乎无法检测到。
- 安全事件的潜在征兆数量一般都很高,比如每天入侵检测系统会报告成千上万条告警信息。
- 对安全事件的相关数据进行正确而有效的分析往往需要高水平的专业知识和丰富

的实践经验。多数组织内，具备这些条件的人很少。

安全事件的征兆可以分为两类：迹象（Indication）和前兆（Precursor）。前兆是指未来可能发生的安全事件的征兆，而迹象是指已经发生或正在发生的安全事件的征兆。迹象的种类太多，以至于无法一一介绍，以下是其中一些例子：

- 某台 FTP 服务器发生缓冲区溢出时网络入侵检测传感器报警。
- 反病毒软件发现某台主机被蠕虫感染时发出告警。
- Web 服务器崩溃。
- 用户抱怨网络速度太慢。
- 系统管理员发现文件名有不寻常字符。
- 用户向求助台报告收到恐吓邮件。
- 某主机记录其日志中的审计配置发生变化。
- 某应用程序的日志记载了来自未知远程系统的多次失败登录尝试。
- 邮件管理员发现有大量可疑内容邮件流入。
- 网络管理员发现网络流量发生不寻常变化。

不要认为安全事件检测只是一种反应式的，有时候组织也可能在安全事件发生之前就检测到有关行为。比如网络入侵检测传感器发现针对一组主机的不寻常端口扫描活动，这很可能就是对某台主机发起拒绝服务攻击的前兆。以下是其他一些有前兆的例子：

- Web 服务器日志显示，有人使用 Web 服务器弱点扫描工具。
- 公开针对组织邮件服务器弱点的一种新黑客攻击。
- 某黑客组织声称要攻击该组织。

不是所有的攻击都可以通过前兆检测到，有的攻击没有前兆，有的攻击的前兆很难被组织发现。如果在攻击之前发现前兆，那么该组织还有机会通过采用自动或人工方法来改变其安全状态来预防安全事件发生。但是大多数情况下，组织可能要在安全事件发生以后才确定采取行动，以求尽快减缓风险。很少情况下，组织可以密切监视某些活动，可能是针对特定主机的连接企图或某些网络流量类型。

3）前兆和迹象的来源

可以通过许多不同的来源来检测前兆和迹象，最常用的有计算机安全软件的告警、日志、公共渠道获取的信息及人。

（1）计算机软件告警：包括基于网络和主机的入侵检测系统、反病毒软件、文件完整性检测软件、第三方监视服务等。

（2）日志：操作系统、服务和应用软件的日志、网络设备日志、蜜罐日志。

（3）公共可获得信息：新弱点及利用信息、其他组织的安全事件信息等。

（4）人：包括组织内部人员及其他组织人员等。

4）安全事件分析

如果能够保证上报来的每一个前兆和迹象的信息都是准确的，那么安全事件的检测和分析将是非常容易的事。但不幸的是，目前这是不可能实现的。例如，当用户抱怨某台服务器无法提供服务，这种情况通常就是不准确的，还有，众所周知，目前的入侵检测系统都会产生大量误报，即不正确的迹象。这些例子说明了造成安全事件的检测和分析如此困难的原因。

对安全事件进行分析和验证是很困难的。以下将提供一些建议，使安全事件的分析更简便有效：

- 描述网络和系统的特征。
- 了解正常行为。
- 使用集中式日志并建立日志保存政策。
- 开展安全事件关联分析。
- 维护和使用信息知识库。
- 利用因特网搜索引擎进行查找。
- 使用数据包监听工具来获取更多信息。
- 考虑数据简化。
- 经验是不可代替的。
- 为没有经验的成员编制一个诊断矩阵。
- 向其他人寻求帮助。

5）安全事件记录

一旦安全事件响应小组怀疑正在发生或已经发生了安全事件，要立即记录有关该安全事件的全部事实。日志簿是一个简单有效的介质方法，但目前个人数字助理（PDA）、笔记本计算机、录音机以及数码相机也可以用于这种目的。把系统事件、电话交谈记录下来并观察其中变化可以使问题处理更有效、更系统并且更少犯错误。从安全事件被发现到处理完毕过程中所采取的每一个步骤都应该加以记录，并注明时间。与安全事件有关的每份文档都应该让安全事件处理人员注明日期并签字。这类性质的信息也可以作为法律诉讼相关证据。如果有可能，事件处理应该至少保持两人一组的工作方式：一个人开展技术工作的同时，另一个人进行日志记录。

安全事件响应小组应该将安全事件状态及其他相关信息一起加以保存记录。为实现这一目的，有必要使用一个应用或数据库系统，以保证能够及时地处理和解决安全事件。比如，安全事件处理人员可能会接到与前一天所解决的安全事件相关的紧急电话，而当时的安全事件处理人员不在现场，通过访问安全事件数据库，事件处理人员可以快速了解安全事件。

安全事件处理小组还应该小心保护与安全事件相关的数据，因为这些数据中经常会包括一些敏感信息，比如被利用弱点方面的数据，最近的安全违反活动及那些可能采取不适当行动的用户。要减少敏感信息被不适当外泄的风险，小组应该保证严格限制对安全事件数据的管理，比如只有经过授权的人员才能访问安全事件数据库。与安全事件相关的电子邮件以及安全事件报告文档应该加密，保证只有发送方和目标收件人才能读懂。

6）安全事件的优先排序

对安全事件处理进行优先排序可能是安全事件处理过程中最关键的一个环节。由于资源的限制，安全事件不应该按照先来先处理的原则进行处理，而应该按照以下两个因素来对安全事件的处理进行优先排序。

- 安全事件当前和潜在的技术影响：安全事件处理人员不仅应该考虑安全事件目前的负面技术影响（比如对数据的未经授权的用户级访问），而且还要考虑在安全事件没有被立即限制时，它未来的可能技术影响。比如，某个蠕虫病毒正在组织的网络

中传播，它当前的影响还非常小，但是在几个小时内蠕虫流量可能导致网络资源被耗尽。

- 受影响资源的关键程度：受安全事件影响的资源（如防火墙、Web 服务器、因特网连接、用户工作站以及应用）对组织的关键程度各不相同。资源的关键程度取决于数据或服务、用户、与其他资源的信任关系和相互依赖程度以及可视性（比如一个公众 Web 服务器相对于一个内部部门的 Web 服务器）。许多组织已经通过业务连续性计划工作或他们的服务等级协定确定了资源的关键性。只要可能，安全事件响应小组就应该获取并重用有关资源关键性方面的有效数据。

7）安全事件的通知

分析安全事件，并对其进行优先排序以后，安全事件响应小组需要通知组织内外部的适当人员。及时的报告和通知可以使相关人员发挥其作用。在目前信息安全威胁的数量巨大、情况复杂的情况下，合作处理安全事件是最好的方法。安全事件响应政策应该包括安全事件报告规定，至少要规定报告对象、报告时间以及报告内容等。

3. 限制、消除和恢复

1）选择限制策略

对安全事件进行检测并分析，并在事件超出控制或造成更大的破坏之前加以限制。对大多数的安全事件都要加以限制，限制的一个必要环节是做出决定（比如关机、从有线或无线网络中断接、断开 Modem 线、禁用某些功能等）。如果已经预先确定了安全事件限制策略和流程，做出决定就容易得多，组织应该在安全事件处理中定义什么样的风险是可接受的，并据此制定策略。

限制策略随着安全事件类型的不同而不同。比如，针对邮件病毒感染事件的限制策略和针对基于网络的分布式拒绝服务攻击的限制策略就很不一样。强烈建议组织要针对各个主要安全事件类型制定单独的限制策略。相关标准要有明确记录，以便快速有效地做出决定。限制策略的选择标准有：

- 资源的潜在破坏和失窃。
- 证据的保存需求。
- 服务的可用性（比如网络连接、对外提供的服务）。
- 执行策略所需的资源和时间。
- 策略的有效性（如部分限制了安全事件、完全限制了安全事件）。
- 解决方案的持续时间（比如紧急工作区需要在 4 小时内拆除、临时工作区需要在 2 周内拆除）。

某些情况下，为了收集更多的证据，有些组织可能会推迟对安全事件进行限制以便对攻击行为加以监视。安全事件响应小组必须先同法律部门协商，以确定这种推延是否可行。如果组织在察觉到系统被破坏后，还允许这种破坏行为继续进行，那么它要对攻击者利用已被破坏的系统来攻击其他系统的后果承担责任。这种推延限制策略是非常危险的，因为攻击者可能提高未经授权的访问级别或很快去破坏其他系统。只有经验丰富的安全事件响应小组在能够监视所有的攻击行为并能迅速切断攻击者的连接的前提下才能使用这一策略。即便如此，推延限制策略所带来的好处往往不及它所带来的风险。

与限制相关的另一个潜在问题是有些攻击在被限制时可能会带来其他破坏。比如一个

被破坏的主机可能运行一个恶意进程，定期 ping 另一台主机，当安全事件处理人员为了限制安全事件而切断该主机与网络的连接时，以后的 ping 命令将无法发挥作用，结果该恶意进程可能将所有数据写到主机的硬盘中。安全事件处理人员不应该仅仅因为主机从网络中断接了，就假定已经防止了对主机的进一步破坏。

2）证据搜集和处理

尽管在安全事件中收集证据的主要理由是解决安全事件，但是这还需要法律行动。这些情况下，要明确记录所有证据，包括被破坏系统是如何得到保留的。应该按照一定的流程来收集证据，这些流程要符合所有适用的法律和条例，并根据与法律人员或适当的执法机构的讨论结果制定出来，这样才能在法庭上被采纳。此外，对证据要随时给予说明，在证据移交过程中，应该在保管链表上对交接详加说明并要有各方的签名，此外还要为所有证据保留一份详细的日志。

3）确定攻击者

在安全事件处理期间，系统拥有者和其他人一般都想知道攻击者是谁。尽管这个信息很重要，特别是当组织希望能对其进行起诉时，但是安全事件处理人员应该将精力集中在对安全事件的限制、消除和恢复上。查询攻击者身份可能是一个耗时而又无效的过程，它可能妨碍小组实现其主要目标：将业务影响减小到最低程度。在识别攻击者过程中最常采取的活动如下：

- 确认攻击者的 IP 地址。安全事件处理方面的新手通常都会把注意力集中在攻击者的 IP 地址上，试图使用 ping、traceroute 或其他一些方法来确认该 IP 地址是不是假冒的。但是，这样做意义不大，最多也只能表明这个地址对应的主机对请求做出了响应。没有响应并不表示这个地址不真实，比如某台主机可能被配置成不响应 ping 或是 traceroute。此外，攻击者的地址可能是动态获得的（比如来自拨号 Modem 池），该地址可能又被分配给其他人。更重要的是，如果 IP 地址是真实的，那么小组 ping 它时反而会让攻击者察觉到组织已经检测到他的活动。如果这是在安全事件被完全限制之前，那么攻击者可能还会制造其他破坏，比如清除硬盘上的攻击证据。在采取地址确认这样的动作时，小组应该考虑并使用其他组织的 IP 地址（如 ISP），这样确认活动的真实源头就对攻击者隐藏了起来。
- 扫描攻击者的系统。有些安全事件处理人员除了用 ping 或 traceroute 来检查 IP 地址之外还会采取更多措施。他们可能会使用端口扫描、弱点扫描工具及其他一些工具来收集更多关于攻击者的信息。比如扫描活动可能会发现系统中有特洛伊木马正在监听，这意味着攻击主机本身已经受到破坏。在使用这些扫描工具之前，安全事件处理人员应该先与组织的法律代表进行讨论，因为这类扫描可能会和组织的政策冲突，甚至触犯法律。
- 使用网络搜索引擎查找攻击者。在大多数攻击中，安全事件处理人员至少会有一些关于攻击者可能身份的一些信息，比如 IP 源地址、电子邮件地址或是 IRC 上的昵称。利用这些数据在因特网上进行搜索可能会搜索到更多的攻击者信息，如有关类似攻击的邮件列表消息，甚至是攻击者的 Web 主页。这些搜索工作并不需要在安全事件被完全限制之前进行。
- 使用安全事件数据库。由几个小组收集来自各个组织的入侵检测和防火墙日志数

据并将它们合并到安全事件数据库中。有些这样的数据库允许人们搜索对应一个特定 IP 地址的记录。安全事件处理人员可以使用该数据库来查看是否有其他组织正在报告来自相同来源的可疑活动。组织也可以检查自己的安全事件追踪系统或数据库来查找相关活动。

- 对攻击者可能的通信信道进行监视。有些安全事件处理人员用来确定攻击者的另一种方法是监视攻击者可能使用的通信信道。比如，攻击者可能聚集在某个 IRC 频道上，吹嘘他们已经篡改了哪些 Web 主页。但是安全事件处理人员应该仅仅将他们得到的这类信息看作是深入调查和证实的潜在线索，而不是事实。

4）消除和恢复

在安全事件被限制之后，就要开始着手消除安全事件的各个组成部分，比如清除恶意代码、禁用违规账号。对有些安全事件，消除工作或者没必要或者要在恢复过程中开展。在恢复过程中，管理员要把系统恢复到正常状态，并且对系统进行加固防止类似安全事件的再次发生。恢复工作通常会涉及以下活动，比如从干净的备份上对系统进行恢复、重建系统、用干净的版本来替换被破坏的文件、安装补丁、更换口令并加强网络边界安全（比如防火墙规则集、边界路由器的访问控制列表）。最好采用更高级别的系统日志或网络监视，作为恢复过程的一部分。一旦某个资源被成功攻击，那么它往往还会再次遭到攻击，或者同一组织中的其他资源可能会遭到类似的攻击。Internet 上有许多用于恢复和保护系统的有用资源。

4. 事件后活动

1）汲取经验

学习和改进是安全事件响应中最重要也是经常被忽略的部分。每个安全事件响应小组都应该不断进步以应对新的威胁、适应新的技术并汲取经验教训。在发生严重安全事件后，许多组织都会举办一次“经验汲取”会议，这对改善安全措施以及安全事件处理过程本身是非常有帮助的。这类会议通过回顾发生何种事件、采取了何种活动来解决问题以及解决程度如何等提供一次机会来对安全事件做出结论。这类会议应该在安全事件发生后的几天内举行。

另一个重要的安全事件后活动是针对每个安全事件创建一个随后的报告，并建立正式的事件年表（包括像系统日志信息这样的时间戳信息），这对将来使用非常有用。事件报告将为今后协助处理类似安全事件提供参考，并可能作为日后进行起诉活动的基础。后续报告应该按照记录保存政策中所规定的时间进行保存。

2）使用收集到的数据

经验汲取活动应该产生与每个安全事件相关的一套主观和客观数据。一段时间后，这些安全事件数据应该在多个方面都能用到。这些数据，尤其是事件总耗费时间和成本可能会被用来说明安全事件响应小组额外资金的合理性。安全事件特征研究可能会揭示出系统安全弱点和威胁，以及安全趋势的变化。这些数据也可以反馈到风险评估过程中，并最终对安全控制的选择和实现提供指导。这些数据同时还可以为安全事件响应小组的成功与否加以度量。如果安全事件数据能够适当收集并合理存放，它应该提供几种对安全事件响应小组成功性的度量方法。

3）证据保存

组织应该建立相关政策对证据保存的时间做出规定，多数组织选择在安全事件结束后

将所有证据保存几个月或几年。在创建政策过程中应该考虑以下因素：

（1）起诉。

如果要对攻击者进行起诉，那么可能需要将证据保存到所有的法律动作结束为止。有些情况下，证据可能会保存几年时间。而且现在看起来没有意义的证据可能在将来变得非常重要。比如，攻击者可能根据之前的攻击中收集到的信息又发起更为严重的攻击，那么来自第一次攻击的证据在解释第二次攻击如何实现时就非常关键。

（2）数据保存。

多数组织都有数据保存政策，规定某些类型的数据需要保存的时间。比如，某个组织规定电子邮件消息最多保存 180 天。如果磁盘映像中包含几千封电子邮件，组织可能不希望此映像的保存期超过 180 天，除非确实有必要。一般记录时间表规定安全事件处理记录应该保存 3 年。

（3）成本。

作为证据存放的原始硬件（如硬盘、遭破坏系统）以及用来保存磁盘映像的硬盘和其他设备对多数组织来讲都不贵。但是，如果组织常年保存着大量的这种设备，那成本就会很高。组织还必须保留专门的计算机，可以使用这些被保存的硬件（如硬盘）和介质（如备份磁带）。

4）安全事件处理核对

针对安全事件各个阶段的处理过程建立安全事件处理核对表，然后，安全事件处理人员使用该核对表来配合特定类型的安全事件。

5）建议

获取在安全事件处理过程中可能有价值的工具和资源。如果安全事件响应小组拥有各种工具和资源，那么就能更为有效地处理安全事件。这些工具和资源包括联系簿、加密软件、网络图、备份设备、计算机犯罪取证软件、端口列表及安全补丁等。

通过保证网络、系统以及应用充分安全来预防安全事件的发生，不仅对组织有好处，而且可以减少安全事件响应小组的工作负担。开展定期风险评估并将已知风险降低到可接受的程度对减少安全事件的数量非常有效。用户、IT 人员及管理层对安全政策和流程的意识也是很重要的。

通过不同类型计算机安全软件产生的报警来识别前兆和迹象。基于网络和主机的入侵检测系统、反病毒软件及文件完整性检测软件都可以对事件的征兆进行检测。每种软件都可以检测到其他类型软件所无法检测到的安全事件。所以，建议同时使用多种计算机安全软件。第三方的监视服务也是很有用的。

为外部组织报告安全事件建立相关机制。有些外部组织希望将安全事件报告给本组织，他们可能认为组织内部有人发起了攻击。组织应该公布一个电话号码及电子邮件地址，使外部组织能通过它们来报告安全事件。

7.4.2　应急计划

1988 年，莫里斯蠕虫以迅雷不及掩耳之势肆虐互联网，导致上千台计算机系统的崩溃，造成数千万美元的损失。这突如其来的灾难，给人们敲响了警钟，面对信息系统遭遇侵害程度的不断增强，对付入侵不仅需要防御，还要能够在事件发生后进行应急响应和处理。1989

年,在美国国防部的资助下,CERT(Computer Emergency Response Team,计算机紧急响应小组)/CC(Call Center)成立。从此应急响应被摆到了人们的议事桌上。CERT 成立以后做了大量工作,但最大的成就就是使应急响应为人们普遍接受。

一般来说,每个使用信息系统的组织都应当有一套应急响应的机制,应急响应机制包括两个环节:应急响应组织和应急计划。

应急响应组织的主要工作是对安全事件与软件安全缺陷进行分析研究,开发与管理安全知识库,并发布安全信息,进行安全事件的紧急处理,同时进行安全管理和应急知识的教育与培训。应急响应组织包括应急保障领导小组和应急技术保障小组。应急保障领导小组的主要职责是领导与协调突发事件与自然灾害的应急处理。应急技术保障小组主要解决安全事件的技术问题,如物理实体和环境安全技术、网络通信技术、系统平台技术、应用系统技术等。

应急计划是指根据不同的突发紧急事件类型和意外情形,预先制定的处理方案与计划。应急计划一般包括执行应急计划的人员、系统紧急事件类型及处理措施的详细说明、应急处理的具体步骤和操作顺序 3 个重要方面。应急计划的目标是在灾难期间当信息系统或普通运行环境不可用时,继续为客户提供服务,遵守规章需求,并继续内部业务。应急操作的实现可以在原始站或备用站上进行。应急事件处理的基本流程和步骤主要包括 7 个重要方面,下面将对各个环节进行详细说明。

1. 安全事件报警

值班人员发现紧急情况,要及时报告。报告要对安全事件进行准确描述并作书面记录。按照安全事件的类型,安全事件呈报条例应依次报告值班人员、应急工作组长以及应急领导小组。如果想进行任何类型的跟踪调查或者起诉入侵者,应先跟管理人员和法律顾问商量,然后通知有关执法机构。一定要记住,除非有执法部门的参与,否则对入侵者进行的一切跟踪都可能是非法的。同时,还应通知有关人员,交换相关信息,必要时可以获得援助。

2. 安全事件确认

应急计划是根据安全事件的类型进行对应的处理的,确定安全事件的类型,以便启动相应的应急计划。一些常见的安全事件类型有:物理实体及环境安全类安全事件,如意外停电、物理设备丢失、火灾、水灾等;网络通信类安全事件,如网络蠕虫侵害等;主机系统类安全事件,如计算机病毒、口令丢失等;应用系统类安全事件,如客户信息丢失等。

3. 启动应急计划

首先要能够找到应急计划,接下来就是要保护现场证据(如系统事件、处理者采取的行动、与外界的沟通等),避免灾害扩大。

4. 恢复系统

首先考虑安装干净的操作系统版本。如果主机被侵入,就应当考虑系统中的任何东西都可能被攻击者修改过了,包括内核、二进制可执行文件、数据文件、正在运行的进程以及内存。通常,需要从发布介质上重装操作系统,然后在重新连接到网络上之前,安装所有的安全补丁,只有这样才会使系统不受后门和攻击者的影响。只是找出并修补被攻击者利用的安全缺陷是不够的。建议使用干净的备份程序备份整个系统,然后重装系统。只配置系统要提供的服务,取消那些没有必要的服务。检查并确信其配置文件有没有脆弱性及该服务

是否可靠。同时安装供应商提供的所有补丁，使系统能够抵御外来攻击，不被再次侵入，这是最重要的一步。并查阅 CERT 的安全建议、安全总结和供应商的安全提示。谨慎使用备份数据，在从备份中恢复数据时，要确信备份主机没有被侵入。恢复过程可能会重新带来安全缺陷，被入侵者利用。最后要修改密码，在弥补了安全漏洞或者解决了安全配置问题以后，建议改变系统中所有的账户的密码。

5. 加强系统和网络的安全

首先根据 CERT 和 UNIX/NT 配置指南检查系统的安全性，并安装所有选择的安全工具。同时，最好使用 Tripwrite、aide 等工具对系统文件进行 MD5 校验，把校验码存储在安全的地方，以便以后对系统进行检查。其次，启动日志、检查或记账程序，将它们设置到准确的级别，并配置防火墙对网络进行预防，然后再重新连接到 Internet。

6. 应急工作总结

召开会议，分析问题和解决方法。会议主要商讨的内容包括 3 个方面：第一，总结教训，从记录中总结出这起安全事件的教训，这有助于检讨自己的安全策略；第二，计算事件的代价，使组织认识到安全的重要性；第三，改进安全策略。

7. 撰写安全事件报告

安全事件报告的主要内容包括安全事件发生的时间、安全事件处理参加的人员、事件发现的途径、事件类型、事件涉及范围、现场记录、事件导致的损失和影响、事件处理过程、使用的技术和工具、经验和教训。

7.5 灾难恢复

信息系统的灾难恢复指的是系统遭遇自然或人为灾害以后，重新启用信息系统的数据、硬件及软件设备，恢复正常运作的过程。简单地说，灾难恢复是灾后恢复操作的能力。灾难恢复计划是涵盖面广泛的业务连续性计划的一部分，其核心是对企业或机构的灾难性风险做出评估、防范，特别是对关键性业务数据、流程予以及时记录、备份和保护。

这里的灾难指的是任何导致信息系统持续一段时间失效的危害，如病毒、黑客、水灾、火灾等。对于信息系统来说，一旦突发灾难，将会在很大程度上造成系统软硬件基础设施、业务数据等的毁灭，要应对突如其来的灾难，保障信息系统的持续服务能力，就需要提供信息系统的灾难恢复功能。美国的明尼苏达大学的一项研究表明：金融业在灾难停机 2 天内所遭受的损失为日营业额的 50%，如果两个星期内无法恢复信息系统，75%的公司将业务停顿，43%的公司将再也无法开业；没有实施灾难备份措施的公司 60%将在灾难后 2～3 年间破产。由此可见，灾难恢复是企业业务持续运作的保障，同时也是企业规避风险、健康发展的要求，更是行业监管政策的要求。自 2000 年以来，我国国务院办公厅以及国信办也持续颁发了一系列关于信息系统灾难备份与恢复的监管政策。

信息系统中的数据根据其存储位置的不同，其安全可以分为两个层面：数据的静态安全与数据的动态安全。数据的静态安全顾名思义，指的是防止存放在数据服务器存储设备上的数据被窃取、修改、删除或破坏。而数据的动态安全是指在数据传输过程中防止信息被

截获或篡改，常用的技术手段及工具包括数据备份、快速恢复、异地存放、远程控制、灾难恢复等技术，所强调的重点在于“保”。目前系统保护技术主要是指数据备份和恢复技术，本节将重点讨论数据分类、数据备份和灾难恢复技术等内容。

7.5.1 数据分类

数据资源是数据中心中最为重要的资源，没有数据的数据中心是没有丝毫意义和作用的。同时数据也是信息系统的核心资产，网络攻击者和别有用心的人攻击网络的主要目的之一是获取敏感数据。因此，对数据资源的管理是一项非常重要的运行管理工作。其中，数据分类是数据资源管理的主要内容之一。

随着数据量的迅速增长，数据中心必须制定切实可行的计划，以便在当今和将来较长的时间内有效地管理和保护这些数据，从而确保这些组织的成功和生存。然而，并非所有信息都是价值相等的。价值特别高的活动的在线数据必须随时可供多个组织和应用程序快速存取。有些数据要求每天 24 小时具有 100%的即时存取能力，不容许停机。有些数据对于某些组织比对于另外一些组织更重要。有些数据会随着时间的推移而改变其价值，而有些数据的存档只是为了偶尔存取或长期存储。

了解数据对于日常业务运作的价值，并了解何种数据需要以多快的速度存取，是信息生命周期管理计划的所有要素的基础，这些要素包括：

- 设计有效的存储基础结构战略。
- 优化存储管理以控制与信息增长和存储利用率相关的成本和复杂性。
- 整合信息存储以使当前投资的信息基础结构变得更高效、更易于管理。
- 规划业务连续性，以便有效管理所有环境下的数据可用性。

数据分类是执行信息生命周期管理计划的任何工作都必不可少的第一步。数据分类也是信息系统实施安全等级保护的基本原则，按照数据的价值的不同划分数据的类别，对不同类别的数据，应实施不同的安全等级保护。

数据分类是一个流程，它定义了一个组织的不同类型数据的性能和可用性特征，并针对每种分类建议了可满足其需要的适当的存储技术。企业（机构）中的数据按逻辑类别分组，以便于实现关键存储目标。

若要制定一个灾难恢复战略或业务连续性规划，则需要按照业务的关键程度对数据进行分类。这样就能够在数据的业务价值和保护这些数据所需的数据恢复措施之间建立适当的联系。若要定义一个资源占用收费模型，则需要按照消耗的存储资源，或按照管理成本对数据进行分类。这将确保各部门的存储负担与其所使用的存储资源量相称。若要制定一个全面的存储战略，则需要根据业务优先级（如首先投放市场、客户宣传等），对数据进行分类。这将确保数据被维护在与其业务优先级相称的适当的存储基础结构上。在设计一个信息存储整合规划时，可能就需要按照物理状态和位置对数据分类。这样就能够发现并消除数据孤岛，并使最重要的数据项更接近其最终用户。

有效的数据分类从确定数据的使用目标开始，例如，制定一个业务连续性计划，为所有部门或一些部门制定资源占用收费计划，或者移动或整合一个数据中心。这决定了如何对数据进行分组或分段，以便最好地实现特定的目标。这一做法希望达到的最终目的是创建一个可操作的模型，它定义了一组有限且可识别的信息，可以以一种能够满足既定业务目标

的方式操作这些信息。

通过数据分类确定关键业务数据是一个长期的过程，随着公司或机构数据的不断增长，必须制定一个对数据进行分类保护的策略，以保证数据保护计划与公司业务同步，下面概括了数据分类的一些方法。

(1) 公开数据。该类是公开发布的数据，需要进行完整性保护。应按第一级用户自主保护级的要求进行安全设计

(2) 一般数据。该类数据的破坏和泄露，将会带来一定的损失，应按第二级，即指导保护级的要求进行安全设计。

(3) 重要数据。该类数据具有重要价值或机密程度，需要进行重点保护，应按照第三级，即监督保护级的要求进行安全设计。

(4) 关键数据。该类数据具有很高的使用价值或机密程度，需要进行特别保护，应按第四级，即强制保护级的要求进行安全设计。

(5) 核心数据。该类数据具有最高使用价值或机密程度，需要进行绝对保护，应按专控保护级的要求进行设计。

若能正确执行，数据分类就可以产生一个模型，这一模型可将具有相似数据管理要求的数据整合到同一逻辑分组中，从而不再需要分别描述各个数据项。然后，可以使用此模型帮助定义变化情形或提供一个框架以便创建分层存储体系结构。

数据分类模型可以为企业或机构增添巨大的价值。有效的数据分类是实施企业或机构数据管理优化战略的坚实基础。数据分类有以下几方面的价值：

(1) 提供了组织中各类数据的清晰景象。

(2) 描述了核心业务职能和相关数据之间的联系。

(3) 展示出数据对于业务来说所具有的经济价值。

(4) 为每一种数据类别设计和制定共享的技术体系结构。

(5) 为每一种数据类别定义一套与存储相关的服务(例如可用性、可恢复性、可管理性、可扩展性和可补充性)。

对于全面实现更广泛的存储相关计划的价值来说，数据分类是一项必不可少的基础工作。将数据分类作为存储相关计划中一个不可缺少的组成部分，收集必要的信息来优化存储环境并使投资得到最大的回报。

应将数据分类看作关键的第一步，它使许多重要的存储管理能力得以实现。适当的数据分类为各层应用程序及其数据确立了服务级别需求，服务级别需求是由适当的技术配置级别提供的。

数据分类的最终目标是最后在企业或机构内部提供一种可操作的数据分组机制。作为其结果产生的数据分类模型接着可以用来围绕当前的企业或机构存储做法构建业务案例，或者用来帮助实施建议的与存储相关的计划。

7.5.2　灾难备份

在信息化程度比较高的行业，如 IT 行业、金融行业等，一旦发生重大安全问题或未知灾难，将直接影响到行业的各项工作，并危及其未来的发展，造成严重的后果。因此，对灾难的未雨绸缪逐渐受到关注，灾难备份也日益受到重视。

灾难备份是指为了降低灾难发生的概率以及灾难发生时或发生以后造成的损失而采取的各种防范措施。为了对灾难进行恢复,灾难备份一般会对数据、数据处理系统、网络系统、基础设施、技术支持能力和运行管理能力进行备份。灾难备份的主要目标是保护数据和系统的完整性,使业务数据损失最少甚至没有业务数据损失。

衡量灾难备份效果的两个主要技术指标是恢复点目标(Recovery Point Object,RPO)和恢复时间目标(Recovery Time Object,RTO)。其中RPO指的是灾难发生时刻与最近一次数据备份时刻的时间间隔,即尚未来得及对数据进行备份导致数据丢失的数据量。主要针对丢失的数据量,代表了数据容灾的指标。为尽可能减少数据丢失,需要建立一个远程的数据存储系统,并对生产系统进行数据的镜像备份。而RTO是指系统从灾难发生到重新启动的时间,代表系统恢复的能力。RTO针对的是服务丢失,是衡量应用容灾的指标,即在数据容灾的基础上,在灾难备份中心建立一套完整的与生产系统匹配的备份应用系统。在灾难发生时,灾难备份中心可以迅速接管业务运行,不仅能最大限度地降低丢失的数据量,而且能最大限度地减少系统恢复时间,保证系统不间断地运行。RPO与RTO二者没有必然的关联性,RTO和RPO的确定必须在进行风险分析和业务影响分析后根据不同的业务需求确定。对于不同企业的同一种业务,RTO和RPO的需求也会有所不同。

根据国际标准SHARE 78的定义,灾难备份技术方案可以根据以下主要方面所达到的程度而分为7个等级(详见表7.1)。

- 备份与恢复的范围。
- 灾难恢复计划的状态。
- 应用站点与灾难备份站点之间的距离。
- 应用站点与灾难备份站点之间的连接方式。
- 数据在两个站点之间传输方式。
- 允许丢失的数据量。
- 灾难备份站点数据更新要求。
- 灾难备份站点可以开始灾难备份工作的能力。

表7.1 灾难备份方案的7个等级比较

级　别	特　点	适用场合
0级:无异地备份	仅在本地进行备份,没有在异地备份数据,未制定灾难恢复计划,成本最低,不具备真正的灾难恢复能力	是所有灾难备份方案的基础,从个人用户到企业级用户都广泛采用
1级:异地备份	将关键数据备份到本地,然后送往异地保存,但异地没有可用的备份中心、备份数据处理系统和备份网络通信系统,未制定灾难恢复计划。这种方案成本较低,但难以管理	在许多中小型网站和中小型企业用户中采用较多。对于要求快速进行业务恢复和海量数据恢复的用户,这种方案是不能够被接受的
2级:热备份站点备份	将关键数据备份并存放到异地,制定相应的灾难恢复计划,备份介质是采用交通运输方式送往异地,在异地有热备份中心,但保存的数据是上一次备份的数据	灾难发生后可能会有几天甚至几周的数据丢失,故不能用于关键数据的灾难备份

续表

级　别	特　点	适用场合
3 级：在线数据恢复	通过网络将关键数据备份并存放至异地，制定相应的灾难恢复计划，有热备份中心，并配备部分数据处理系统及网络通信系统。特点是用电子数据传输取代交通工具传输备份数据，从而提高了灾难恢复的速度	由于备份站点要保持持续运行，对网络的要求较高，因此成本相应有所增加
4 级：定时数据备份	在第 3 级方案的基础上，利用备份管理软件自动通过通信网络将部分关键数据定时备份至异地，并制定相应的灾难恢复计划	对备份管理软件和网络设备的要求较高，导致成本增加。还不能满足关键行业对关键数据容灾的要求
5 级：实时数据备份	在前几级的基础上使用硬件镜像技术和软件的数据复制技术，关键应用使用了双重在线存储，减少了数据丢失量，降低了业务的恢复时间	既能保证当前交易正常进行，又能实时复制交易的数据到异地，是目前应用最广泛的方案
6 级：零数据丢失	利用专用的存储网络将关键数据同步镜像至备份中心，数据在本地和异地都要进行确认，恢复速度最快，实现零数据丢失	投资大，适合资金实力雄厚的大型企业和电信企业，适合交易较少或非实时交易的关键数据系统，目前采用此方案的用户不多

根据信息系统数据中心与备份中心的距离远近，可以分为同城灾备和异地灾备两种灾难备份方案。同城灾难备份方案是在同城或相近区域内建立两个数据中心：一个为生产中心，负责日常生产运行；另一个为灾难备份中心，负责在灾难发生后的信息系统正常运行。这种方案由于生产中心与灾难备份中心的距离比较近，比较容易实现数据的同步镜像，保证高度的数据完整性和数据零丢失。同城灾难备份方案一般用于防范火灾、建筑物破坏、供电故障、计算机系统以及人为破坏引起的灾难。而异地灾难备份一般是在两个较远的（100km 以上）的城市分别建立生产中心和灾难备份中心，实现远距离的灾难备份。异地灾难备份不仅可以防范火灾、建筑物破坏等可能遇到的风险隐患，还能够防范战争、地震、水灾等风险。异地灾难备份需要更多的投资。

同城灾难备份和异地灾难备份各有所长。为达到最理想的防灾效果，在保证信息系统性能的前提下，可考虑采用同城和异地各建立一个灾难备份中心的解决方案。

灾难备份是一项非常复杂的工作和任务，需要用到多方面的技术与设备，而灾难备份系统的核心技术是数据备份技术和数据的存储备份技术。

（1）数据备份技术。

一个完整的灾难备份系统主要由数据备份系统、备份数据处理系统、备份通信网络系统和完善的灾难恢复计划组成。在灾难备份系统建设中，数据备份是关键，如何将数据（包括系统、应用和业务等数据）完整、实时地复制到灾难备份中心，是灾难备份系统建设中首先要考虑的重点。

- 基于磁盘系统的灾难备份技术：采用硬件数据复制技术，借助磁盘控制器提供的功能，通过专线实现物理存储器之间的数据交换。包括同步数据复制模式和异步数据

复制模式两种数据复制模式。

- 基于软件方式的灾难备份技术：其特点是与操作系统平台无关，对应用程序透明，此方式通过通信网络实现数据在两个不同地点的实时备份。

(2) 数据的存储备份技术。

数据的存储备份技术是灾难备份的另一个核心技术。其中，存储优化是提高灾难备份系统性能的重要指标之一。目前，比较通用的存储优化技术有直接连接存储(Direct Attached Storage，DAS)、网络连接存储(Network Attached Storage，NAS)和存储区域网络(Storage Area Network，SAN)。

灾难备份建设的基本流程和步骤如下：

(1) 建立灾难备份专门机构。

实施灾难备份应由董事会或高级管理层决策，指定高层管理人员组织实施。由科技、业务、财务、后勤支持等与灾难备份相关的部门组成专门机构，主要职责包括分析灾难备份需求，制定灾难备份方案；确定工程预算，监督工程实施；明确各部门的职责，协调各部门关系；对灾难恢复计划定期进行测试和评估；对测试和评估的结果进行审核和存档并做出相应的改进。

(2) 分析灾难备份需求。

重要信息系统灾难备份需求分析应包括对数据处理中心的风险分析和对重要信息系统的业务分析，以确定灾难恢复目标。数据处理中心风险分析的内容包括分析数据处理中心的风险，如物理安全，数据安全，人为因素，已有的备份和恢复系统、基础设施脆弱点，数据处理中心位置，关键技术点等；明确防范风险的技术与管理手段；确定需要采取灾难恢复的类型，如灾难备份中心的距离，数据备份方式和频率等。业务分析的内容包括各项业务停业将造成的损失，须考虑流失客户、损失营业额、企业形象、法律纠纷、社会安定因素等；每项业务停顿的最大容忍时间；各项业务的恢复优先级；各项业务的相关性；可接受的交易丢失程度。灾难恢复目标主要有确定恢复业务品种范围及优先级、确定灾难备份中心及服务界面的恢复时限、确定需要恢复的服务网点和服务渠道。

(3) 制定灾难备份方案。

灾难备份方案分为多个等级。一个完整的灾难备份方案的设计基于灾难备份需求分析所得出的各业务系统灾难恢复目标，它可能涉及多个级别的应用，并且需要考虑技术手段、投资成本、管理方式等多方面因素，主要内容包括：

① 数据备份方案。

根据灾难备份需求分析所确定的业务恢复时间和交易丢失程度确定对数据备份的要求，按照应用的重要级别、最大停顿时间、数据传输量、最大数据丢失度、数据相关性、应用相关性等确定数据备份的方案。

② 备份处理系统。

灾难备份应根据重要信息系统灾难备份需求配置相应的备份处理系统。根据数据备份方案确定相应的数据备份所需的主机、存储、网络、系统、软件等；根据灾难恢复应用对主机系统、磁盘系统、磁带备份、打印及外围设备的需求确定硬件配置；根据服务界面的范围、备份网络拓扑结构、网络传输速率需求、网络切换方式、网络恢复时间要求以及本地的网络通信状况确定网络配置。

③ 灾难备份中心建设。

灾难备份中心是配备各种资源用以在灾难发生时接替数据处理中心运行的计算机处理中心，重要信息系统可采用自行建设、联合建设和租用商业化灾难备份中心的模式。

④ 规程与管理制度。

重要信息系统需要制定有关灾难备份与灾难恢复的各项规程和管理制度，同时修改数据处理中心原有规程和管理制度以确保灾难恢复的成功，这些规程和制度包括数据备份日常管理制度、备份数据保存制度、灾难备份切换流程、灾难备份系统变更管理规程以及人力资源规程等。

(4) 实施灾难备份方案。

实施灾难备份方案的主要目标是按照所制定的灾难备份方案，完成灾难备份工作。实施过程中，要严格按照灾难备份方案的要求和内容进行，要落实相应的规章制度，要应用灾难备份方案，建设并运行灾难备份中心。

(5) 制定灾难恢复计划。

制定灾难恢复计划的主要目的是规范灾难恢复流程，使重要信息系统在灾难发生后能够快速地恢复数据处理系统运行和业务运作；同时重要信息系统可以根据灾难恢复计划对其数据处理中心的灾难恢复能力进行测试，并将灾难恢复计划作为相关人员的培训资料之一。

(6) 保持灾难恢复计划持续可用。

在灾难恢复计划制定后，为保证计划的可用性和完整性，需要制定变更管理流程、定期审核制度和定期演练制度。

① 工作底稿。

对重要信息系统现有的数据处理中心信息处理系统配置、恢复时间、恢复范围等进行确定以形成工作底稿，详细列明数据处理中心需要进行灾难备份的主机、附属设备、系统软件、数据库软件、应用软件、网络设备配置清单；同时列明数据处理中心服务对象的终端设备、网络及附属设备的硬件配置、系统版本和应用软件清单。

② 变更流程。

重要信息系统应建立变更机制以控制数据处理中心和灾难备份中心的变更，所有的变更对灾难恢复计划的影响均应得到评估。这些变更包括操作系统变化、新增应用软件、硬件配置更改、网络配置或路由更改等。因此，必须要制定完善的变更管理流程，保证灾难恢复计划的修改与变更事项同步进行。

③ 维护和评估。

灾难恢复计划需要由各相关部门定期进行审核和更新以保证其完整和有效，灾难应变小组负责人负责组织审核工作，各相关部门参与。内部审核工作应至少每六个月进行一次，审核的结果应报主管领导，并对不足之处加以改善。外部审计机构可以接受主管部门委托，对重要信息系统的内部控制状况进行审计，也可以接受聘请对重要信息系统的内部控制做出审计评价；外部审计机构发现重要信息系统内部控制的问题和缺陷，应当及时向主管部门报告。

④ 测试和演练。

灾难恢复计划常常因为错误的假设、疏忽或设备及人员的变更而不可用，因此需要经常

的测试以保证其及时和有效。测试的另一目的是让灾难恢复队伍和有关的人员熟悉灾难恢复计划。

灾难备份是灾难恢复的基础，是围绕着灾难恢复所进行的各类备份工作，灾难恢复不仅包含灾难备份，更注重的是业务恢复。

7.5.3 灾难恢复方案的选择

灾难恢复是一个复杂而艰难的过程，同时也是一个耗资巨大的项目，因此，在利益最大化的考虑之下，选择最优的灾难恢复方案就显得尤其重要。IBM 公司认为所有的灾难恢复方案都必须考虑 5 大因素，即灾难覆盖面、恢复速度、恢复程度、可用的技术及方案总成本。综上所述，可以用图 7.3 表示。

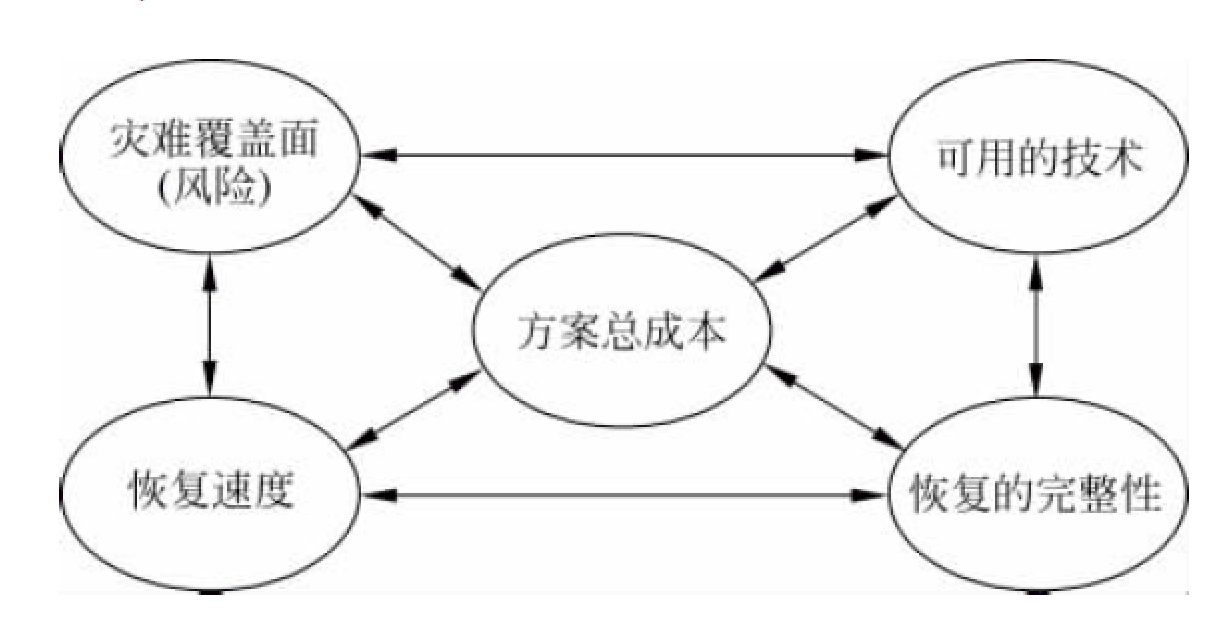


图 7.3 灾难恢复方案选择标准

根据国际标准 SHARE78 的定义，灾难恢复解决方案可以根据系统恢复各方面所要达到的程度分为 7 个等级，即从低到高有 7 种不同层次的灾难恢复解决方案，详见表 7.1。可以根据系统数据的重要性以及所需要恢复的速度和程度，来设计选择并实现所需要的灾难恢复计划。

在选择灾难恢复解决方案时，非常重要的一点是解决方案所需的投资在 IT 商业价值中应占切实可行的部分，希望用较少的投资换取更多的利益——灾难恢复解决方案的投资一定要少于灾难本身带来的财政损失。

按照下面的 4 个关键目标，为一个企业选择解决方案时，就更容易做出决定。

1. 恢复时间目标(RTO)

RTO 是指在灾难发生后，从系统业务停顿之刻开始，到系统业务恢复运营之时，此两点之间的时间段。RTO 代表了系统的恢复能力，一般来说 RTO 越短，由灾难造成的业务损失就越小，而灾难恢复方案的成本就越高；反之，RTO 越长，由灾难造成的业务损失就越大，而灾难恢复方案的成本就越低。恢复成本与恢复时间的关系如图 7.4 所示。对一个确定的 RTO 支持程度可以用来衡量业务连续性技术较好，反之较低。

2. 恢复时间点目标(RPO)

RPO 是指一个过去的时间点，当灾难或紧急事件发生时，数据可以恢复到的时间点，RPO 代表了业务所能容忍的数据丢失量。一般来说恢复时间点目标 RPO 越高，丢失的数据量就越少，灾难造成的业务损失就越小，而灾难恢复方案的成本就越高；反之，恢复时间点目标 RPO 越低，丢失的数据量越多，灾难造成的业务损失越大，而灾难恢复方案的成本则

越低。恢复时间和数据丢失造成的损失的关系如图 7.5 所示。

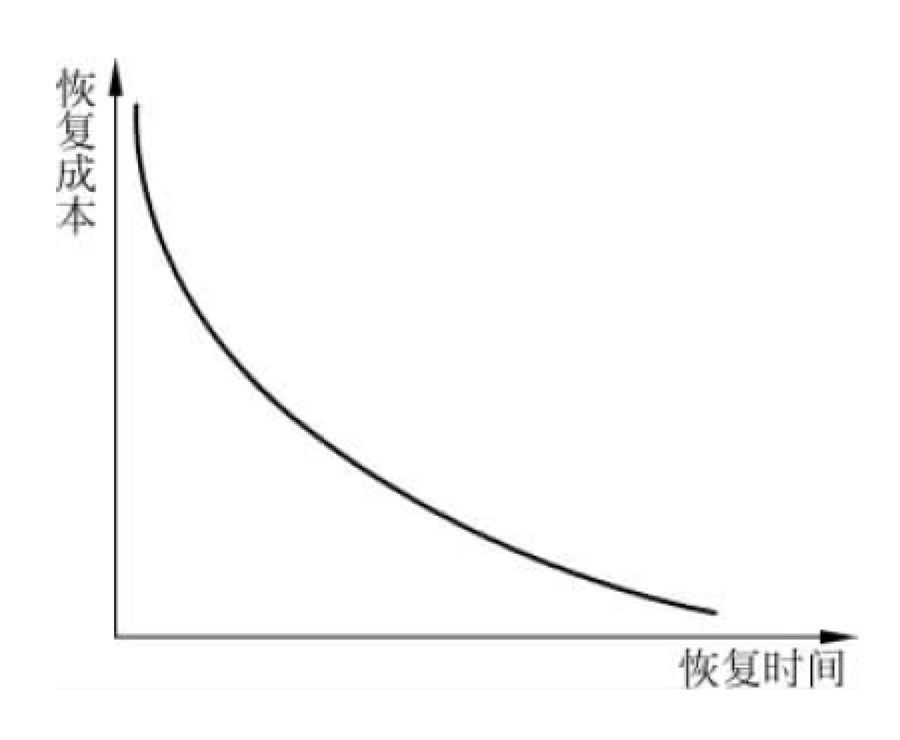


图 7.4　恢复成本和恢复时间的关系

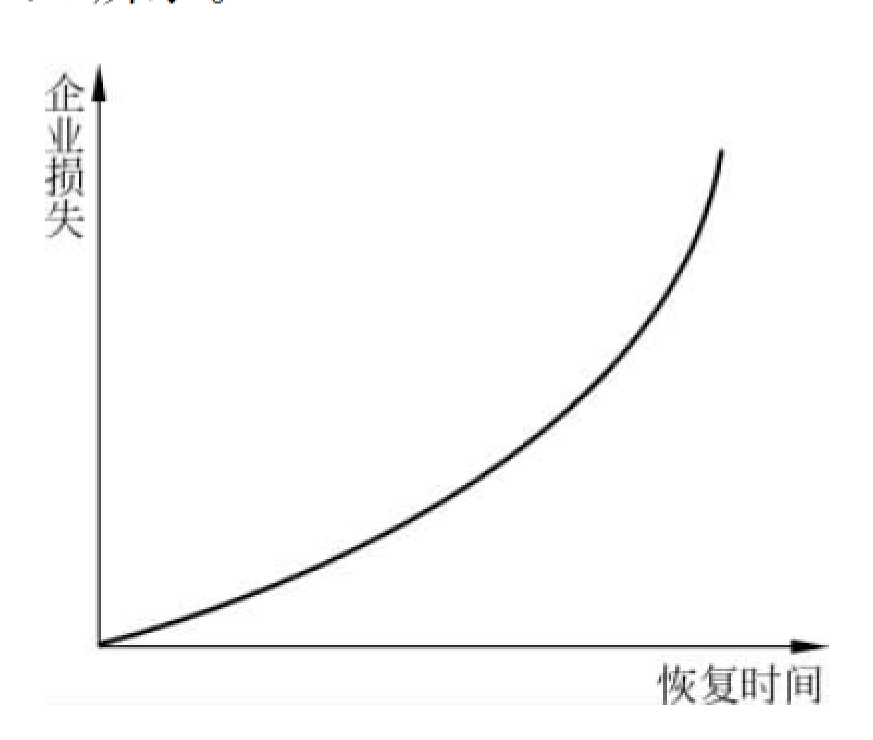


图 7.5　企业损失和恢复时间的关系

3. 降级操作目标(Degraded Operations Objective,DOO)

灾难恢复不仅仅考虑 RTO 和 RPO,还考虑降级操作时间。降级操作目标 DOO 是指在恢复完成后到防止第二次灾难的所有保护恢复以前的时间。在只有一个数据中心和一个备份中心的情况下,当灾难发生时,业务切换到备份中心,要尽快恢复和重建数据中心,减少降级操作时间。

4. 网络恢复目标(Network Recovery objective,NRO)

NRO 即网络切换所需要的时间。

恢复方案一定是在全面衡量了实施费用、维护费用、灾难对财政的影响,并对业务影响进行了分析后而得出的一个综合方案。

每一层灾难恢复方案的恢复时间通常是指恢复处理业务服务所需的安装时间。然而在现实的灾难中,需要对其他更多的事项进行考虑。例如,有些业务可以容忍较长时间的停机服务,但要求一旦业务开始就需要使用最多的实时数据;有些业务必须在尽可能短的时间内恢复服务,而不考虑数据的实时性;还有一些既需要在最短的时间内恢复服务,也需要最多的实时数据。

通过评估具体场地的实际灾难恢复需求,为恢复计划开好头。灾难恢复方案的成本是根据客户需要在多快的时间内恢复数据以及业务处理服务中断将带来的损失这两点得出的。恢复数据所需的时间越少,业务处理服务中断的时间就越短,所需的方案成本就越高。另一方面,业务处理中断的时间越长,由此带来的损失就越大。最优的方案就是,方案成本曲线和业务停止带来的损失的曲线的交集——成本—时间窗口。如图 7.6 所示。

7.5.4　成本效益分析

所谓成本效益分析就是将投资中可能产生的成本与效益归纳起来,利用定量或定性的分析方法计算成本和效益的比值,从而判断该投资项目是否可行。成本效益是一个矛盾的统一体,二者互为条件、相伴共存又互相矛盾、此增彼减。从事物发展规律来看,任何事情都存在成本效益。成本大致可划分为两个层次:一个是直接的有形的成本;另一个是间接的无形的成本。效益也包含两个层次:一个是直接的有形的效益,另一个是间接的无形的效益。

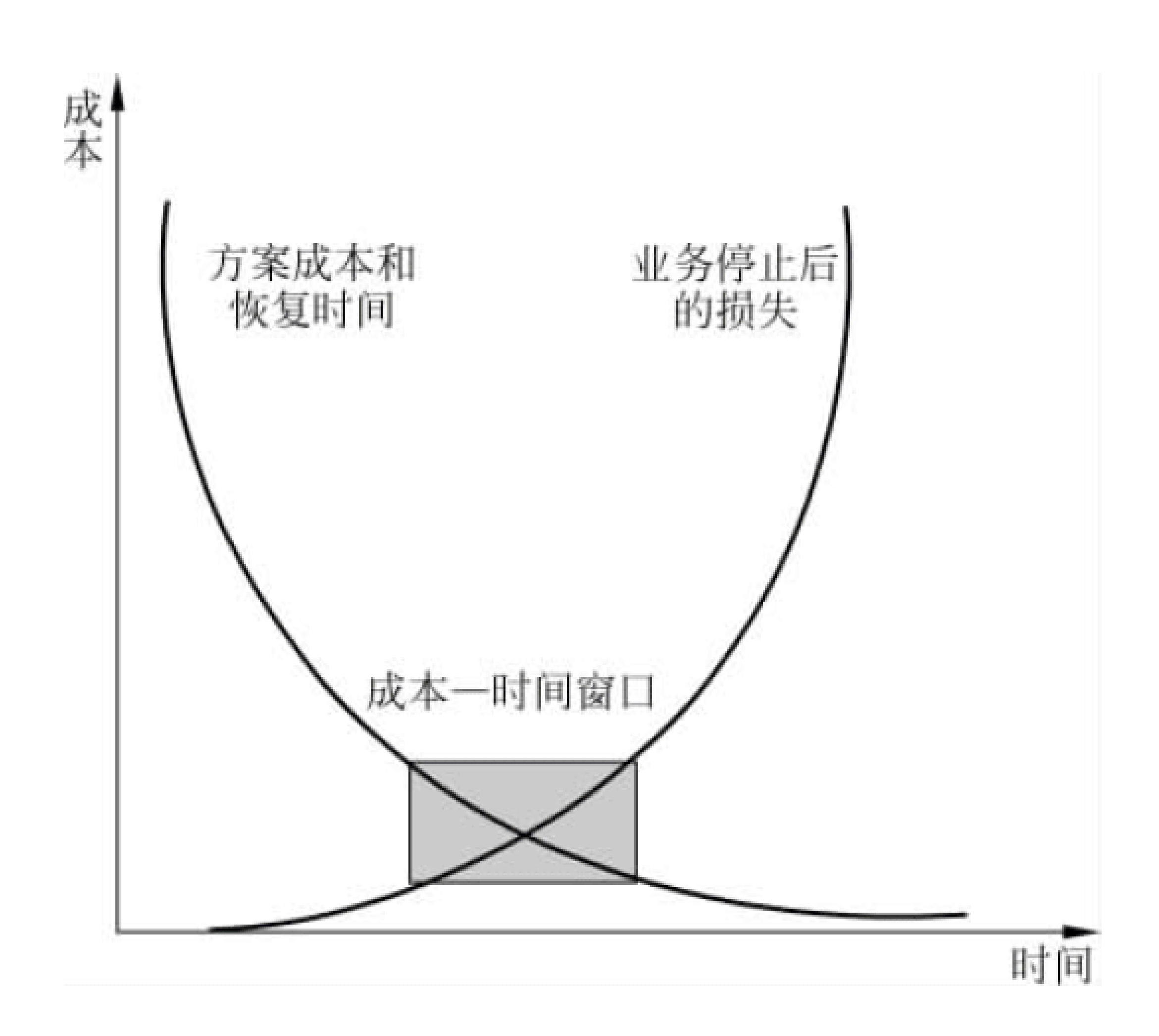


图 7.6　灾难恢复成本—时间窗口图

例如，某公司要购买一批新车，希望这些车辆能给更多的顾客，以更快的速度运送更多的货物。关键的问题是这笔投资将增加多少利润，借助传统的财务方法，有关部门可以进行相当精确的预测，包括一次性购买成本、每年新增的人员开支、每年新增的维护费用、每年新增的折旧和每年新增的预期收入等。可以据此计算出每年的投资回报率以及收回投资的时间等。如果需要，还可以评价同样的投资在银行、股票或者其他投资项目中的回报测算，并最终给出投资评估的建议，这样就更容易通过预算审查。然而，IT 投资却没这么简单。很少有 CIO 能对 IT 投资给出类似的数据。

Alinean 顾问公司总裁兼 CEO、评估顾问 Thomas Pisello 说："在今天的经济环境下，CIO 承受着巨大的压力。他们要说明预算的合理性，还要对那些并不明显的回报进行评估。"让 IT 价值显现出来，需要一种合理的评估方法，把 IT 投资对单位的财务贡献识别出来。采用过评估方法的 CIO 们说，IT 评估模型可以帮助他们在 IT 和商业战略之间、技术驱动和股东价值之间建立直观的联系，而且方便和 CFO 的沟通。这样，可以帮助他们最终获得更多的 IT 投资，并且花在更有价值的地方。

1. 成本效益分析的方法

灾难恢复是系统建设的重要组成部分，通常以项目的方式进行。我们可以按照项目管理的成本效益分析方法对灾难恢复建设进行成本效益分析。但是灾难恢复建设又有自己的特点，信息系统灾难恢复建设内容包含灾难备份系统、支持维护体系和灾难恢复管理制度等，它比通常的信息系统建设更为全面。灾难恢复建设的价值实现是在灾难发生时体现的，具体的体现时间是不确定的，这和绝大部分信息系统建设项目从投产时就产生效益有较大的区别。因此，对于灾难恢复建设的效益分析也与通常的信息系统建设有很大的不同。

传统成本效益分析中通常只需要分析成本和收益，在新的成本效益分析体系中，加入了对项目风险的关注。

项目效益＝收益－成本

项目效益＝(收益－成本)×风险系数(成功概率)

通过成本效益分析，可以在不同的方案中进行比较和选择，选择对单位最有利的投资

方案。

在信息技术系统项目中，常用的成本效益分析方法可以划分为 3 类：传统财务方法、定性方法（也叫启发式方法）和概率方法。不管采用哪种方法，评估的最终目的是唯一的，即在 IT 投资和单位盈利之间建立直接的关联。

传统财务方法是成本效益分析中历史最悠久也是最常用的一类分析方法，它脱胎于投资项目分析，将 IT 项目作为一种投资来分析成本的构成和效益的产出，计算具体的量值并依此给出比较结果。方法间的不同之处在于对成本、效益和项目风险的估算方式。在信息技术领域比较常用的是总体拥有成本（TCO）。TCO 方法的主要优点是不单纯评估项目的静态成本，同时考虑整个产品服务生存周期内的所有费用，不仅包括开发、采购、运输、安装和调试的显性成本，还包括修理、维护和操作人员等可能发生的隐性成本。对那些喜欢 TCO 方法“铁面无私”特点的技术经理们，TCO 已经成为他们生活的重要内容。TCO 在现行成本对比分析方面很出色，是评估和控制 IT 开销的良好手段。但是，TCO 不能评估风险，也不能就如何把技术与战略、竞争性商业目标结合起来提供指导。

定性方法有时被称为启发式方法，旨在用主观的、定性的指标评价人员和流程的价值，对定量方法是有益的补充。对于大部分单位而言，信息技术系统的投入不能带来直接的经济利益，而传统财务方法往往很难精确衡量收益部分，可采用主观评价体系，通过记分卡、配比组合和综合评价等方式对收益和风险进行综合评价。

概率论方法运用统计和数学模型测量一定概率范围内的风险。概率论方法对于希望得到量化结果的用户是很具有吸引力的。它通过运用统计样本和数学模型计算隐性收益和风险，为使用者提供较精确的数量结果。但是，概率论方法必须得到统计样本和数学模型的支持，而对于特定的单位而言，要得到一个可用的较精确的结果，统计样本和数学模型都必须定制，除了对于专业技能的要求外，无论从时间上还是成本上都是相当可观的，这限制了概率论方法的运用。

到底应该选择哪种价值评估方法，评估者除了考虑方法本身的特点外，还应当考虑评估者自己以及单位运作方式的影响。

下面对灾难恢复成本分析进行说明。

（1）灾难恢复成本＝恢复速度×恢复的完整性×防范风险的范围和等级。

其中，恢复速度是指在业务发生中断后重新恢复并提供相关服务所需的时间，一般以 RTO 表示，恢复速度越快，所需成本越高。恢复的完整性包括恢复功能的完整性、恢复数据的完整性和恢复能力的完整性。恢复的功能越完整，恢复过程中数据丢失越少，恢复后的处理能力越大，则成本越高。防范风险覆盖的范围越大，风险类别越多，防范风险等级越高，则成本越高。

（2）灾难恢复成本效益合理区间。

在灾难发生时，业务中断所造成的损失是一个与时间有关的变量，如图 7.6 所示。随着业务中断时间的延长，损失大小呈指数曲线上升。根据国外的统计数字，一个单位如果发生业务中断超过 14 天，那么它会在一年后倒闭的可能性有 70%。而恢复成本却随着恢复时间指标要求的下降而呈指数曲线下降。在这两条曲线的交叉点附近就是所要追求的恢复时间目标，即恢复成本的合理区间。恢复成本的合理区间就是图 7.6 中的成本时间窗口。

这两个灾难风险的成本效益分析模型包含的因素并不完整，具体的参数和曲线也很难

量化,但是为方案选择和合理性可行性分析提供了一个可以借鉴的方法。

综上所述,成本效益分析中包括成本、效益和风险3个重要因素,前面介绍的几种成本效益分析的方法,在成本、效益和风险的分析过程中各有特点,没有哪一种方法是最好的,应该根据实际的情况选择最合适的方法。

2. 成本效益分析的内容

在分析灾难恢复项目建设的成本效益时,应该关注以下几个方面。

1) 成本

在进行成本分析时,可以借鉴总体拥有成本的方法。IT环境日益增长的复杂程度使得TCO模型面向的是一个由分布式的计算、服务台、应用解决方案、数据网络、语音通信、运营中心以及电子商务等构成的IT环境。TCO同时也度量这些设备成本之外的因素,如IT员工的比例、特定活动的员工成本和信息系统绩效指标等,终端用户满意程度的调查也经常被包含在TCO的标杆之中。这些指标不仅支持财务上的管理,同时也对其他与服务质量相关的改进目标进行合理性考察和度量。在大多数TCO模型中,以下度量指标中的基本要素是相同的。

(1) 直接成本,包含在传统的IT预算中,包括软硬件、运营、管理等。

(2) 间接成本,由IT用户产生的成本,包括宕机时间、终端用户运营等。

通过TCO的分析可以发现,IT的真实成本平均超出购置成本的5倍之多,其中大多数的成本并非与技术相关,而是发生在持续进行的服务管理的过程中。TCO会产生一个与单位成本相关的由货币度量的数值。许多单位希望能将自己的成本信息与其他同类单位进行比较。事实上,这些数据只有当被用来与其他在TCO方面作为行业标杆的单位进行比较,或与本单位之前的度量结果进行比较得出取得进步(或退步)的结论时才能发挥其真正的作用。

灾难恢复项目的成本来源于以下几个方面。

(1) 备用基础设施建设。

作为提供灾难恢复服务的基础设施,在功能区划分、环境控制、安保监控、电力保障、通信保障和地理位置选择等方面都有较高的要求。不论是采取租用还是自建方式,备用基础设施的选择、建设或租赁、装修等费用都是必须被考虑的。这些支出基本是一次性的。

(2) 数据备份系统。

数据备份系统是灾难恢复项目的核心服务内容,是保证数据安全性、完整性和有效性的关键环节。相关的存储设备、专用网络设备、主机设备、备份软件和应用软件等的设计、采购、安装、集成和培训费用也是灾难恢复项目成本必不可少的一个组成部分。这些支出除了数据复制线路的租用外,其他基本上是一次性的。

(3) 备份数据处理系统。

备份数据处理系统是在灾难发生后,灾难备份中心能够继续提供数据处理服务的必要保证。根据灾难恢复项目的建设目标的不同,备份数据处理系统建设并不是灾难恢复项目必需的组成部分。备份数据处理系统根据目标和具体应用体系的不同可能包含主机、存储、专用网络、系统软件和应用软件等设备。这些费用基本上是一次性的。

(4) 备用网络系统。

备用网络系统主要是用来支持在生产中心或生产网络发生故障后,最终用户访问灾难备份中心或生产中心的备用网络。备用网络系统建设包括网络设备、线路铺设、线路租用和

管理软件等的安装、集成和培训等。根据灾难恢复建设的需求和目标的不同，可能不包含备用网络系统的建设。其中设备和软件的采购安装费用基本上是一次性的，但是备份网络线路的租用将是长期连续性的。

(5) 技术支持能力。

灾难恢复系统是一个建设门类齐全的项目，包含了基础设施工程，主机和网络等各种硬件，备份管理、操作系统、数据库和应用系统等各种软件。保障这些基础设施和软硬件系统的长期稳定运行，长期可靠的技术支持是必不可少的。技术支持能力可以通过购买厂商服务的方式获得，也可以通过建立技术支持团队来获取，更多的情况下，是两种情况的综合。不论采取什么方式取得长期可靠的技术支持能力，都必然需要费用上的付出，而且这种支出将是连续性的。

(6) 运行维护管理。

能够长期有效地保证对生产系统的恢复功能，是灾难恢复系统的基本使命。为了达到这个目标，灾难恢复系统必须有一个高效、可靠的运行维护体系。灾难恢复系统的数据要与生产系统保持一致，在生产系统发生技术架构调整、软硬件配置调整、应用系统程序变更时灾难恢复系统也必须做出相应调整。作为一套长期处于运行就绪状态或运行准备状态的系统，还必须对运行过程中发生的问题进行及时的处理以保证灾难恢复系统的随时可用。专业运行维护管理人员须提供 5×8 或 7×24 不间断的服务，这是一个连续性的成本投入。

(7) 灾难恢复预案制定。

灾难恢复预案是根据用户需求目标，结合已经制定的灾难恢复策略，在灾难发生时具体指导相关人员执行恢复动作的计划。灾难恢复预案的制定和执行跨越了从主机、网络、存储到电力、空调和消防等多个技术学科，跨越了从单位主管、信息技术到财务、后勤支持等多个部门。灾难恢复预案制定的本身就是一个复杂的系统工程，必须组建专门的团队或者由第三方的专业公司提供咨询服务。同时，灾难恢复预案还必须随着单位的发展、技术的进步、人员的调整、策略的改变定期或不定期地进行更新调整。不论采取什么方式，投入的人员与时间也是灾难恢复项目必须考虑的成本因素。

根据以上分析可采用 TCO 的方式，全面考虑一次性投入和在可预期的时间内的连续性投入，可以对灾难恢复项目在一定时间周期内的成本构成和金额得出较可靠的结论。

2) 效益

在成本效益分析中，效益的构成有两个组成部分，效益＝成本的减少＋收益的增加。

在灾难恢复项目的建设过程中，效益分析是一件比较困难的事情。首先，效益分析中收益的增加部分往往是难以度量的预期值，比如单位信用度的提升、用户忠诚度的提高和单位长期可持续发展能力的提升等，这些价值的提升往往带有不确定性，具体的价值也很难量化估算。其次，成本的减少效果不明显，从显性的效果来看还会带来经营成本的增加(连续性的投入)。但是，如果将单位的业务中断损失作为成本的一个组成部分，那么灾难恢复项目能够带来的损失减少的效果是显而易见的。在数理统计中，有一条重要的统计规律：假设某意外事件在一次实验中发生的概率为 $P(P>0)$，则在 n 次实验中至少有一次发生的概率为：$P_n=1-(1-P)^n$。由此可见，无论概率 P 多么小，当 n 越来越大时，P_n 越来越接近 1，从而说明事故将来必定发生。在单位长期风险不受控制的情况下，长期风险损失的累积爆发完全可以将一个单位拖入万劫不复的深渊。对于灾难恢复项目可能给单位带来的收益及

其关键性程度可以通过业务影响分析得出。

业务影响分析描述了哪些业务对于单位的生存至关重要,这些业务能够容忍多大程度的中断或停止响应以及发生中断后会对单位造成多大的损失等。通过这些描述,可以认识甚至量化单位的长期风险损失的范围、程度和概率,以及通过灾难恢复项目可以在多大程度上避免这些损失。

在进行业务影响分析的时候必须注意,对于业务中断带来的损失的大小和范围是一个和中断时间相关的变数。随着业务中断时间的延长,业务中断所带来的损失呈指数曲线上升,当业务中断时间超过某个阈值,单位将面临倒闭的风险。

3) 风险

任何项目都存在失败的风险,灾难恢复项目也是一样,有很多这样的案例可以证明。对单位需求把握得不准确,对风险防范范围掌握得不全面,运行维护和技术支持投入力量不足,备份恢复技术方案存在缺陷,没有恢复预案或者没有足够的演练,都可能导致在灾难性事件真正发生时灾难恢复系统不能起到应有的作用。项目风险的大小对于项目成本效益分析也是至关重要的要素,可以认为:项目真实成本=项目可见成本×风险系数。风险系数越大,项目的真实成本就越高,风险系数的比较对于不同项目实现方式的成本效益的比较分析具有重要的参考意义。

灾难恢复项目的风险可能来自以下几个方面。

(1) 认知风险。

认知风险是对项目威胁最大的风险,如果对项目的需求和目标发生认知错误或者偏差,那么整个项目无论如何运作都不可能取得最后的成功。在灾难恢复的建设过程中,需求分析、灾难恢复策略制定阶段是可能存在认知风险最大的阶段。借鉴其他机构或者专业厂商提供的成熟经验和方法可以最大限度地减少认知风险。

(2) 技术风险。

在开发实施阶段,应尽量选择灾难恢复领域中成熟的技术、产品和技术实现方案,以降低可能的技术风险。灾难恢复项目对可靠性的要求极高,是整个信息系统的最后一道防线。如果可能,应事先进行技术和设备的模拟测试,将技术风险减至最低。

(3) 操作风险。

在项目的实施阶段,应保持对项目的控制,包括成本控制、计划控制和质量控制,及时发现差异、跟踪差异并解决差异,避免项目的进度和质量失控而威胁项目的成功。

(4) 外部风险。

灾难恢复、业务连续性在很多国家都已经形成了标准、规范、行业准入制度甚至是国家法律的要求。灾难恢复项目的建设目标和成果必须符合相关的规范和法律要求(部分海外上市公司应同时遵循国外的相关法律法规要求)。在项目的规划期间充分了解所在地、本行业的相关法律法规要求也是灾难恢复项目避免外部风险的必要举措。

7.5.5 灾难恢复过程

灾难恢复是一个周而复始、持续改进的过程,主要包括 4 个重要阶段。

1. 灾难恢复需求的确定

灾难恢复的需求分析一般从以下几个方面考虑:

（1）威胁与风险。

识别信息系统面临的自然的和人为的威胁，识别信息系统的脆弱性，分析各种威胁发生的可能性并定量或定性描述可能造成的损失，识别现有的风险防范和控制措施。通过技术和管理手段，防范或控制信息系统的风险。依据防范或控制风险的可行性和残余风险的可接受程度，确定对风险的防范和控制措施。

（2）资产价值：标识信息系统的资产价值。

（3）业务中断的影响。

对组织的各项业务功能及各项业务功能之间的相关性进行分析，确定支持各种业务功能的相应信息系统资源及其他资源，明确相关信息的保密性、完整性和可用性要求。应采用定量或定性的分析方法，对各种业务功能的中断造成的影响进行评估。其中，定量分析是以量化方法，评估业务功能的中断可能给组织带来的直接经济损失和间接经济损失；定性分析是运用归纳与演绎、分析与综合以及抽象与概括等方法，评估业务功能的中断可能给组织带来的非经济损失，包括组织的声誉、顾客的忠诚度、员工的信心、社会和政治影响。

（4）业务的关键性、时效性。

（5）灾难恢复目标的确定

根据威胁与风险分析和业务中断的影响，确定灾难恢复的目标，包括灾难恢复范围、系统中断可容忍的时限（恢复点目标）、系统多久能恢复（恢复时间目标）以及各项业务恢复的优先级和相关性等。

2. 灾难恢复策略的制定

灾难恢复策略是一个单位为了达到灾难恢复的需求目标而采取的途径，它包含实现的计划、方法和可选的方案。灾难恢复策略是指导整个灾难恢复建设的纲领性文件，描述了灾难恢复需求的实现步骤和实现方法。但是，灾难恢复策略不等同于具体的技术方案，灾难恢复策略的制定是原则性、方向性的。

在制定灾难恢复策略时应该注意可行性分析，可行性包括成本合理性、技术手段可实现以及资源可获取等。

灾难恢复策略的制定包含以下两个很重要的要素：

（1）灾难恢复资源要素。

支持灾难恢复各个等级所需的资源（以下简称“灾难恢复资源”）可分为 7 个要素（详见表 7.2）。

表 7.2　灾难恢复资源的 7 个要素

要　素	组　成
数据备份系统	硬件、软件、介质
备用数据处理系统	备用计算机、外设、软件
备用网络系统	备用通信设备、线路
备用基础设施	场所、组织、设备、辅助设施等
专业技术支持能力	硬件、系统及应用软件分析处理能力及管理协调能力
运行维护管理能力	对运行环境、系统、安全、变更的管理能力
灾难恢复预案	组织管理、应急响应、恢复与继续运行、重建及回退、预案的保障和管理

(2) 成本效益分析原则。

根据灾难恢复目标,按照灾难恢复资源的成本与风险可能造成的损失之间取得平衡的原则(以下简称"成本风险平衡原则")确定每项关键业务功能的灾难恢复策略,不同的业务功能可采用不同的灾难恢复策略。

灾难恢复策略由灾难恢复资源的获取方式和灾难恢复能力等级组成。其中灾难恢复资源的获取方式有数据备份系统、备用数据处理系统、备用网络系统、备用基础设施、专业技术支持能力、运行维护管理能力、灾难恢复预案。

另外,灾难恢复资源的要求包括以下几个方面:

(1) 数据备份系统。组织应根据灾难恢复目标,按照成本风险平衡原则,确定数据备份的范围、数据备份的时间间隔、数据备份的技术及介质、数据备份线路的速率及相关通信设备的规格和要求。

(2) 备用数据处理系统。组织应根据关键业务功能的灾难恢复对备用数据处理系统的要求和未来发展的需要,按照成本风险平衡原则,确定备用数据处理系统的数据处理能力、与主系统的兼容性要求及平时处于就绪还是运行状态。

(3) 备用网络系统。组织应根据关键业务功能的灾难恢复对网络容量及切换时间的要求和未来发展的需要,按照成本风险平衡原则,选择备用数据通信的技术和线路带宽,确定网络通信设备的功能和容量,保证灾难恢复时,最终用户能以一定速率连接到备用数据处理系统。

(4) 备用基础设施。组织应根据灾难恢复目标,按照成本风险平衡原则,确定对备用基础设施的要求,包括与主中心的距离要求、场地和环境(如面积、温度、湿度、防火、电力和工作时间等)要求、运行维护和管理要求。

(5) 技术支持能力。组织应根据灾难恢复目标,按照成本风险平衡原则,确定灾难备份中心在软件、硬件和网络等方面的技术支持要求,包括技术支持的组织架构、各类技术支持人员的数量和素质等要求。

(6) 运行维护管理能力。组织应根据灾难恢复目标,按照成本风险平衡原则,确定灾难备份中心运行维护管理要求,包括运行维护管理组织架构、人员的数量和素质、运行维护管理制度等要求。

(7) 灾难恢复预案。组织应根据需求分析的结果,按照成本风险平衡原则,明确灾难恢复预案的整体要求、制定过程的要求、教育、培训和演练要求以及管理要求。

3. 灾难恢复策略的实现

1) 灾难备份系统技术方案的实现

技术方案的设计:根据灾难恢复策略制定相应的灾难备份系统技术方案,包含数据备份系统、备用数据处理系统和备用的网络系统。技术方案中所设计的系统应获得同主系统相当的安全保护,并且要具有可扩展性。

技术方案的验证、确认和系统开发:为确保技术方案满足灾难恢复策略的要求,应由组织的相关部门对技术方案进行确认和验证,并记录和保存验证及确认的结果。按照确认的灾难备份系统技术方案进行开发,实现所要求的数据备份系统、备用数据处理系统和备用网络系统。

系统安装和测试:按照经过确认的技术方案,灾难恢复规划实施小组应制定各阶段的

系统安装及测试计划，以及支持不同关键业务功能的系统安装及测试计划，并组织最终用户共同进行测试。确认以下各项功能的正确实现：

- 数据备份及数据恢复功能。
- 在限定的时间内，利用备份数据正确恢复系统、应用软件及各类数据，并可正确恢复各项关键业务功能。
- 客户端可与备用数据处理系统正常通信。

2）灾难备份中心的选择和建设

选址原则：选择或建设灾难备份中心时，应根据风险分析的结果，避免灾难备份中心与主中心同时遭受同类风险。灾难备份中心还应具有方便灾难恢复人员或设备到达的交通条件，以及数据备份和灾难恢复所需的通信、电力等资源。灾难备份中心应根据资源共享、平战结合的原则，合理地布局。

基础设施的要求：新建或选用灾难备份中心的基础设施过程中，计算机机房应符合有关国家标准的要求，工作辅助设施和生活设施应符合灾难恢复目标的要求。

3）技术支持能力的实现

组织应根据灾难恢复策略的要求，获取对灾难备份系统的技术支持能力。灾难备份中心应建立相应的技术支持组织，定期对技术支持人员进行技能培训。

4）运行维护管理能力的实现

为了达到灾难恢复目标，灾难备份中心应建立各种操作和管理制度，用以保证数据备份的及时性和有效性，并且备用数据处理系统和备用网络系统应确保处于正常状态，并与主系统的参数保持一致，同时要保证系统具有有效的应急响应、处理能力。

5）灾难恢复预案的实现

灾难恢复的每个等级均应按具体实现要求制定相应的灾难恢复预案，并进行落实和管理。

4. 灾难恢复预案的制定、落实和管理

1）灾难恢复预案的制定

（1）制定原则。

- 完整性：包括灾难恢复的过程、数据和资料。
- 易用性：恢复计划中的语言、图表（适于紧急情况下使用）。
- 明确性：灾难恢复的资源、内容、步骤并明确落实到人。
- 有效性：满足灾难恢复需要，保持系统和人的同步更新。
- 兼容性：与其他灾难恢复预案体系有机结合。

（2）制定过程。

灾难恢复预案制定的过程如下：

- 起草。参照灾难恢复预案框架，按照风险分析和业务影响分析所确定的灾难恢复内容，根据灾难恢复等级的要求，结合组织其他相关的应急预案，撰写出灾难恢复预案的初稿。
- 评审。组织应对灾难恢复预案初稿的完整性、易用性、明确性、有效性和兼容性进行严格的评审。评审应有相应的流程保证。
- 测试。应预先制定测试计划，在计划中说明测试的案例。测试应包含基本单元测

试、关联测试和整体测试。测试的整个过程应有详细的记录,并形成测试报告。

• 修订。根据评审和测试结果,对预案进行修订,纠正在初稿评审过程和测试中发现的问题和缺陷,形成预案的报批稿。
• 审核和批准。由灾难恢复领导小组对报批稿进行审核和批准,确定为预案的执行稿。

2）灾难恢复预案的教育、培训和演练

为了使相关人员了解信息系统灾难恢复的目标和流程,熟悉灾难恢复的操作规程,组织应按以下要求,组织灾难恢复预案的教育、培训和演练:

• 在灾难恢复规划的初期就应开始灾难恢复观念的宣传教育工作。
• 应预先对培训需求进行评估,开发和落实相应的培训或教育课程,保证课程内容与预案的要求相一致。
• 应事先确定培训的频次和范围,事后保留培训的记录。
• 预先制定演练计划,在计划中说明演练的场景。
• 演练的整个过程应有详细的记录,并形成报告。
• 每年应至少完成一次有最终用户参与的完全演练。

3）灾难恢复预案的管理

保存与分发——经过审核和批准的灾难恢复预案,应:

• 由专人负责保存与分发。
• 具有多份副本在不同的地点保存。
• 分发给参与灾难恢复工作的所有人员。
• 在每次修订后所有副本统一更新,并保留一套,以备查阅,原分发的旧版本应予销毁。

维护和变更管理——为了保证灾难恢复预案的有效性,应从以下方面对灾难恢复预案进行严格的维护和变更管理:

• 业务流程的变化、信息系统的变更、人员的变更都应在灾难恢复预案中及时反映。
• 预案在测试、演练和灾难发生后实际执行时,其过程均应有详细的记录,并应对测试、演练和执行的效果进行评估,同时对预案进行相应的修订。
• 灾难恢复预案应定期评审和修订,至少每年一次。

7.6 安全审计

计算机技术、电子信息技术与通信技术的完美结合,改变了人类的生产、生活、学习及娱乐的方式,继而造就了一个新的时代——信息时代。在这个新的时代中,人们对数字信息系统的依赖程度正逐渐超过对物理世界的依赖。然而这个虚拟的世界确实十分脆弱,随着人们对它们依赖程度的增加,不安全感也随之增加。信息受到来自外部或内部以及主动或被动的各种攻击的影响,对系统的安全性要求也逐步提高。信息受到的威胁及其本身的脆弱性要求对系统安全方案中的功能提供持续的评估,这就是安全审计。

概括来说,安全审计应当具备以下几项功能:

- 记录关键事件。
- 对潜在的攻击者进行威慑或警告。
- 为系统安全管理员提供有价值的系统使用日志，帮助管理员及时发现入侵行为和安全漏洞，帮助安全管理员对系统安全进行加强和改进。
- 为安全官提供一组可供分析的管理数据，用于发现何处有违反安全方案的事件，并可以根据实际情形调整安全政策。

根据审计对象的不同，安全审计可以分为操作系统的审计、应用系统的审计、设备的审计及网络应用的审计。通常，审计的关键部位有对来自外部攻击的审计、对来自内部攻击的审计、对电子数据的安全审计等。

美国国家标准 Trusted Computer System Evaluation Criteria 给出的安全审计的定义是："一个安全的系统中的安全审计系统，是对系统中任一或所有安全相关事件进行记录、分析和再现的处理系统。它通过对一些重要的事件进行记录，从而在系统发现错误或受到攻击时能定位错误和找到攻击成功的原因，并且是事故后调查取证的基础，当然也是对信息系统的信息保证。"

可以看出，信息系统安全审计是对系统记录和活动的独立评审和考核，以测试系统控制的充分性，确保与既定策略和操作规程相一致，有助于对入侵活动进行评估，并指出系统控制策略和程序的变化。

安全审计机制是一种很有价值的安全管理机制，可以通过事后的安全审计来检测和调查安全策略执行的情况以及安全遭到破坏的情况。安全审计机制是一种事后监督机制，用来检查用户行为是否符合安全政策，帮助发现系统存在的安全漏洞及安全漏洞可能被利用的方式和可能造成的后果，最后根据历史记录追查系统安全破坏者的责任。

安全审计机制主要应实现以下几个目标：

- 能够详细记录所有访问行为的相关数据，并检查安全保护机制的实施结果。
- 能够发现任何具有超越自身规定权限的用户及定位其越权行为。
- 可以发现和定位用户为越过安全机制而进行的反复性尝试行为，并采取相应措施。
- 能够提供证据以表明发生了越过系统安全机制的行为或企图。
- 能够帮助发现和排除系统存在的安全漏洞。

如果系统受到破坏，可以帮助进行损失的评估和系统的恢复。

安全审计需要安全报警报告功能来检测出安全的泄露或可疑事件的发生，并将这些情况报告给操作员或管理员；安全审计需要安全审计跟踪中与安全有关的记录信息，以及从安全审计跟踪中得到的分析和报告信息。审计日志和记录被视为一种安全机制，而分析和报告则被视为一种安全管理功能。

安全审计工作的流程是：收集来自内核和核外的事件，根据相应的审计条件，判断是否是审计事件。对审计事件的内容按日志的模式记录到审计日志中。当审计事件满足报警阀的报警值时，则向审计人员发送报警信息并记录其内容。当事件在一定时间内连续发生，满足逐出系统阈值，则将引起该事件的用户逐出系统并记录其内容。审计人员可以查询、检查审计日志以形成审计报告。检查的内容包括审计事件类型、事件安全级、引用事件的用户、报警、指定时间内的事件以及恶意用户表等。

7.6.1 安全警报

认证、访问控制、机密性和完整性等这些安全服务都是为了防止发生安全泄露。然而，不能保证这些服务总能够正常运行。由于各种攻击行为及系统本身的脆弱性的存在，系统总是会有安全泄密的风险。因此，需要一种能够检测出安全泄露或可疑事件发生的工具。安全警报的主要功能就是监督可疑用户，取消可疑用户的权限，调用更强的保护机制，去掉或修复故障网络或系统的某个组成部件。

从安全审计的定义可以看出，安全审计和安全警报是不可分割的。安全审计由各级安全管理机构实施并管理，并且仅仅在制定的安全策略范围内使用。它允许对安全策略的充分性进行评价，帮助检测安全违规行为，对潜在的攻击者进行威慑或警告。但是，安全审计不直接阻止安全违规行为。安全警报是由一个人或进程发出的警告，以指示发生了异常情况，可能需要及时的行动。安全报警的目的是报告实际的或明显的违背安全的企图、报告各种安全相关的事件，包括"正常"事件以及报告达到一定门限后触发产生的事件。

一个与安全相关的事件会触发一个安全警报，原理上，任何网络或系统部件都能够检测出该事件。在管理模型中，检测事件的部件是受管对象。安全警报通过 M-EVENT-REPORT 通知给管理系统。

安全警报报告功能标准（ISO/IEC 10164-1）描述了 M-EVENT-REPORT 调用中所传递的信息。受管信息定义（ISO/IEC 10165-2）中详细说明了交换中所使用的正确抽象语法。

安全警报报告中传递的参数分为 3 类，涵盖了调用标识符、模式、受管对象类、受管对象事例、事件类型、事件时间、当前时间、通知标识符、相关的通知、额外的信息、额外的文本、安全警报原因、安全警报的严重性、安全警报检测器、使用服务的用户和服务的提供者等。

事件类型和安全警报原因的组合表明了警报的原因。这些原因包括完整性破坏、违规操作、物理入侵、安全服务、机制的侵犯和时间区域的侵犯等。

安全警报的安全参数指明了由初始受害客体发现的警报意义，受害客体所发现的有关系统的警报可能是系统的完整性受到威胁，或者系统安全性被损害，再或者检测到违反安全并且重要的或不太重要的信息或机制已经遭到损害，又或者受害客体根本不相信系统的安全性受到威胁。

安全警报检测器参数是标识检测警报条件的实体，使用服务的用户参数标识那些请求服务从而导致警报发生的实体。服务提供者参数标识那些提供服务从而导致警报发生的实体。

安全报警的产生是检测到任何符合已定义报警条件的安全相关事件的结果，这可能包括达到预定义阈值的情况，有些事件需要立即采取矫正行动，而另一些事件则可能需要进一步调查研究，以便确定是否采取行动。

支持安全审计和报警服务需要多种功能：

（1）事件甄别器，提供对事件的初始分析并且确定是否将该事件转发给审计记录器或报警处理器。

（2）事件记录器，将接收到的消息生成审计记录，且把该记录存入作为安全审计线索。

（3）报警处理器，产生审计消息，同时产生合适的行动以响应一个安全报警。

（4）审计分析器，检查安全审计线索，如果合适就生成安全警报和安全审计消息。

(5) 审计跟踪审查器,在一个或多个安全审计线索外再产生安全审计报告。

(6) 审计提供器,按照某些规则提供审计记录。

(7) 审计归档器,将安全审计的线索部分归档。

安全审计和报警过程包括以下几个阶段:

(1) 检测阶段——与安全相关的事件将会受到检测,包括确定已经发生可能与安全相关的事件。

(2) 甄别阶段——做出初始辨别,确定是否需要将该事件记录在该安全审计线索中,或是否需要产生报警。

(3) 报警处理阶段——发布一个安全处理警报或安全审计消息。

(4) 分析阶段——将一个安全相关事件,与在以前检测到并且由日志记录在安全线索里的事件,以及被确定的行动过程一起纳入上下文背景进行评估。

(5) 聚集阶段——将分布式安全审计跟踪记录汇集成单个安全审计线索。

(6) 报告生成阶段——从安全审计线索中产生出审计报告。

(7) 归档阶段——将安全审计跟踪记录转移到该安全审计跟踪的档案中。

7.6.2　审计日志

审计日志是记录信息系统安全状态和问题的原始数据。理想的日志应当包括全部与数据以及系统资源相关事件的记录,但这样付出的代价太大。为此,日志的内容应当根据安全目标和操作环境单独设计。典型的日志内容有:

(1) 事件的性质。数据的输入和输出、文件的更新(改变或修改)、系统的用途或期望。

(2) 全部相关标识。人、设备和程序。

(3) 有关事件的信息。日期和时间,成功或失败,涉及因素的授权状态,转换次数,系统响应,项目更新地址,建立、更新或删除信息的内容,使用的程序,兼容结果和参数的检测,侵权步骤等。对大量生成的日志要适当考虑数据的保存期限。

日志审计在国外通常叫做日志管理(Log Management,LM),是信息安全审计技术里面比较重要的一项技术手段,与行为审计是相辅相成的审计手段。通过日志审计,协助系统管理员在受到攻击或者发生重大安全事件后查看系统或网络日志,从而评估系统或网络配置的合理性、安全策略的有效性,追溯分析安全攻击轨迹,并能为实时防御提供手段。目前,审计日志仍然面临着各种技术挑战,如日志量巨大、日志格式和内容复杂及日志自身安全性保证等。

对信息系统日志的分析和审计就是对操作系统、系统应用或用户活动所产生的一系列的计算机安全事件进行记录和分析的过程。待审计的用户活动按各自的性质不同,被视为不同的审计事件,审计事件是系统审计用户动作的最基本单位。系统管理员可以有选择地设置对哪些用户、哪些操作(命令或系统调用)及对哪些敏感资源的访问等需要审计,事件的类型、用户的身份、操作的时间、参数和状态等构成一个审计记录记入审计日志。系统管理员可查看和分析审计日志,检查系统中有无危害安全性的活动。

对于一个日志审计系统,从功能组成上至少应该包括信息采集、信息分析、信息存储、信息展示 4 项基本功能。

(1) 信息采集功能:系统能够通过某种技术手段获取需要审计的日志信息。对于该功

能,关键在于采集信息的手段种类、采集信息的范围、采集信息的粒度(细致程度)。

(2) 信息分析功能：是指对于采集到的信息进行分析、审计。这是日志审计系统的核心,审计效果好坏直接由此体现出来。在实现信息分析的技术上,简单的技术可以是基于数据库的信息查询和比较；复杂的技术则包括实时关联分析引擎技术,采用基于规则的审计、基于统计的审计、基于时序的审计,以及基于人工智能的审计算法等。

(3) 信息存储功能：对于采集到的原始信息以及审计后的信息都要进行保存、备查,并可以作为取证的依据。在该功能的实现上,关键点包括海量信息存储技术以及审计信息安全保护技术。

(4) 信息展示功能：包括审计结果展示界面、统计分析报表功能、告警响应功能、设备联动功能等。这部分功能是审计效果的最直接体现,审计结果的可视化能力和告警响应的方式、手段都是该功能的关键。

7.6.3 安全关联

安全审计事件关联分析是在一个比原始审计记录更高的层次上对安全审计数据进行的分析。根据是否需要先验知识,可以把事件关联算法分为两类：有指导关联算法和无指导关联算法。所谓有指导关联算法指的是在先验知识的指导下,完成整个事件关联过程。而无指导关联算法不需要先验知识的帮助而完成事件关联的整个关联工作。需要先验知识的算法,可以归类为基于规则的方法；无须先验知识的算法依据其实现技术分为基于概率统计和基于数据挖掘的方法；此外,有些文献提出,在关联分析的过程中,引入除审计信息以外的系统状态等信息可以提高分析的准确率,我们把此类方法归为基于辅助信息的方法。

1. 基于规则的方法

1) 基于攻击序列模板

基于攻击序列模板的关联方法是最早用于报警事件关联行为研究的一种方法,攻击序列模板也就是先验知识,它的一般形式是：$E=e_1 \text{ op } e_2 \text{ op}\cdots\text{op } e_i \text{ op}\cdots\text{op } e_n$。其中 e_i 为报警事件,op 为 e_i 和 e_j 之间不同的关系运算符。在整个报警事件序列中,不同报警事件的发生隐含着一个时序关系,即 e_{i+1}是 e_i 的后继。

2) 基于因果关系

基于因果关系的事件关联方法的先验知识一般表示为一个三元组(Attack,Prerequisites,Consequences)。其中,Attack 表示攻击动作名,Prerequisites 表示攻击发生的前提条件,Consequences 表示攻击发生后所造成的影响。基于因果关系的关联算法的中心思想就是用攻击 att_i 发生后的后续结果去匹配攻击 att_j 发生的前提条件,如果能够全部匹配或部分匹配成功,则表明攻击 att_i 和 att_j 之间具有因果联系,从而可将两者进行关联。基于单个攻击因果关系的事件关联方法是现在研究最多的一种关联方法。

基于因果关系的方法通过比较先发生报警信息的行为结果和后发生报警信息的行为的先决条件,能够准确灵活地对两个报警信息进行关联。它不仅可以发现已知攻击场景报警信息之间的因果关系,而且可以适应攻击者可变的攻击模式,发现未知攻击场景。这种方法的缺陷在于因果关系的定义过于复杂,以至于它还只是一种离线检测,将其运用于实时的分析中还有待于进一步的研究。

2. 基于概率统计的方法

1）基于贝叶斯分类器的关联方法

首先定义一个观察空间 o 为 o_i，$o_i \in V(1 \leqslant i \leqslant n)$，其中 V 是 o_i 的值域。基于统计，设先验概率为：$p(o_i | s_j) = P(O = o_i | S = s_j)$ $(1 \leqslant j \leqslant m, 1 \leqslant i \leqslant n)$。

由攻击导致的观察值的分布是可以知道的，根据贝叶斯理论，可以计算出它的后验分布：

假设有观察：

$$p(s_j \mid o_i, q_k) = \frac{p(o_i, q_k \mid s_j) \cdot p(s_j)}{p(o_i, q_k)}$$

如果两个空间是独立的，即一个观察空间的事件不会影响另一个观察空间的事件，有：

$$p(s_j \mid o_i, q_k) = \frac{p(s_j \mid o_i) \cdot p(s_j \mid q_k)}{p(s_j)}$$

只要确定就有可能导致现在观察事件的攻击，用下面的公式来比较不同攻击场景的可能性。

$$\frac{p(s_j \mid o_i, q_k)}{p(s_l \mid o_i, q_k)} = \frac{p(o_i, q_k \mid s_j) \cdot p(s_j)}{p(o_i, q_k \mid s_l) \cdot p(s_l)}$$

在很多情况下，两个概率是不可知的，必须假设有同样的概率分布，在这种假设下，上式中先验概率能作为一个选择方法来决定攻击场景。多级随机事件的关系能用贝叶斯网络来表示。一个贝叶斯网络是非循环图，其中每个节点都是随机变量，一个节点概率以一点的条件概率来计算。概率关联很难获得先验概率和条件概率，因此这种方法在现实生活中不太可用。

3. 基于相似度函数

基于相似度函数的关联算法把报警事件定义为一个实体，单个报警事件内容的描述为一个向量，通过定义的相似性函数来计算事件 e_1 与关联队列中的 e_2 之间的相似度，如果当前发生的报警事件其与已发生的报警事件之间的相似度大于预定义的阈值，则其与相似度比较大的事件实体完成关联，否则创建新的关联队列。概率报警关联方法较好地处理了报警的冗余关系，但是概率报警关联方法对不同报警类使用相似性矩阵预先定义，然后进行关联，在表达能力上具有很大的局限性。

4. 基于数据挖掘的方法

基于数据挖掘的方法很多，下面就以基于时间序列分析的关联方法为例进行详细说明。

基于时间序列分析的关联方法引入了时间序列分析的预测方法。首先定义时间间隔 T，然后把该时间间隔划分成 N 份，并利用聚类方法把发生在时间段 i 内的报警事件聚合成事件 A_i，从而产生报警事件集合 $\{A_1, A_2, \cdots, A_n\}$。把事件 $A_i(1 \leqslant i \leqslant n)$ 定义为时间序列分析中的时间序列变量，然后引入 AR 模型：

$$y(k) = \sum_{i=1}^{p} \theta_i y(k-i) + e_0(k)$$

和 ARMA 模型：

$$y(k) = \sum_{i=1}^{p} \theta_i y(k-i) + \sum_{i=1}^{p} \beta_i x(k-i) + e_0(k)$$

并利用公式：

$$g=\frac{(R_0-R_1)/p}{R_1/(T-2p-1)}\sim F(p,T-2p-1)\left(其中\ R_0=\sum_{k=1}^{T}e_0^2(k),R_1=\sum_{k=1}^{T}e_1^2(k)\right)$$

计算新发现的报警事件所对应的事件序列变量 $y(k)$ 和最近发生的报警事件所对应的时间变量 $x(k)$ 之间的 g 值，如果 $x(k)$ 与 $y(k)$ 之间的 g 值最大，则 $y(k)$ 所对应的报警事件与 $x(k)$ 所对应的报警事件具有最大的关联可能性，从而完成事件关联的整个过程。

5. 基于辅助信息的方法

以上是主要的关联分析方法，关联分析还有一个方面是合成带外信息。MZDZ1231 使用形式化数据模型在报警关联过程中处理外部信息。它处理 4 种不同的信息类型：被监视系统的信息、已知漏洞信息、安全工具信息(漏洞扫描器和入侵检测系统)和安全工具产生的信息，如扫描和报警。它使用关系数据库存储网络入侵检测系统和扫描器的信息以及 ICAT 漏洞信息。模型十分灵活并提供了许多报警会聚方法，如相同事件产生的会聚，引用同一漏洞，属于相同 TCP/IP 会话的事件以及基于时间关系等方法。

7.6.4 贝叶斯推理

贝叶斯推理是由英国学者贝叶斯发现的一种归纳推理方法，后来的许多研究者对贝叶斯方法在观点、方法和理论上不断地进行完善，最终形成了一种有影响的统计学派。

贝叶斯推理是在经典的统计归纳推理——估计和假设检验的基础上发展起来的一种新的推理方法。与经典的统计归纳推理方法相比，贝叶斯推理在得出结论时不仅要根据当前所观察到的样本信息，而且还要根据推理者过去有关的经验和知识。贝叶斯推理的问题是条件概率推理问题，这一领域的探讨对揭示人们对概率信息的认知加工过程与规律，指导人们进行有效的学习和判断决策都具有十分重要的理论意义和实践意义。

贝叶斯模型推理的基础是贝叶斯定理，该定理描述如下：

$$p(\theta\mid y)=\frac{p(\theta)p(y\mid\theta)}{p(y)}$$

其中，θ 为模型参数，y 为自观测数据，$p(\theta)$ 为参数的先验概率密度函数。$p(y|\theta)$ 为似然函数，$p(\theta|y)$ 为参数的后验概率密度函数，$p(y)$ 为统计得到的概率值，为常数。

在贝叶斯推理中，$p(\theta)$ 表示在未获得测量数据之前对模型参数分布的认识，主要来源于以往的数据、经验和主观判断等。$p(y|\theta)$ 代表模型参数拟合测量数据的程度，越大表示拟合效果越好，反之越差。$p(\theta|y)$ 表示获得测量数据后模型参数的分布规律，即在统计反演意义下的反问题的解。

贝叶斯推理分为 3 个步骤：

(1) 基于未知参数的所有先验信息确定一个先验概率密度函数。

(2) 找到能够反映模型参数和测量数据之间关系的一个似然函数。

(3) 对后验概率密度函数抽样，进而获得参数的估计值。

似然函数的构造对贝叶斯推理的结果有很大的影响，一般可以人为测量误差服从正态分布 $\varepsilon\sim N(\mu,\sigma^2)$，此时似然函数为：

$$p(y\mid\theta)=\frac{1}{(2\pi\sigma)^{\frac{n}{2}}}\exp\left[-\frac{\left(\frac{d(\theta)-y-\mu}{\sigma}\right)^{r}\left(\frac{d(\theta)-y-\mu}{\sigma}\right)}{2\sigma^2}\right]$$

其中，n 为矩阵中参数的格式，是通过计算获得的后验概率密度函数。然而由于 $d(\theta)$往往比较复杂或模型的空间维数较大，因此后验概率密度函数非常抽象，而且很难直观地表现出来。为了获得估计值，应选取适当的抽样方法，使采样结果接近后验密度函数的概率密度函数。

7.6.5　审计报告

审计人员在审计业务终了以后，要将审计结果加以综合归纳，根据审计证据，提出审计意见，做出审计结论，向审计主管机关和被审单位送交书面报告。这种书面报告，就是审计报告。审计报告既是审计人员对整个审计工作的总结，也是评价信息系统状况的书面证明。

审计报告模式一般采用系统主动提供与被动提供两种方式。系统主动提供就是在系统中加入控制时间，要求系统在特定的时间完成对特定时段审计结果信息的提取、整理与分析；被动提供是用户依据系统提供的审计报警信息或根据自己发现的问题信息向系统提出报告请求，系统根据提出的请求信息给出相应的审计报告。

审计报告的内容主要涉及系统的简要信息、审计结果的简单数理统计、危险等级与事件模式、用户以及工作站相关信息等。在给出简要信息的基础上根据现有的信息安全知识设定系统安全参数来推断当前系统的安全状态，并根据数据分析结果提出相应的安全防范措施或建议。

根据以上介绍，可以总结出安全审计报告中应该包括的内容如下：

(1) 总体评价系统当前的安全级别，应该给出当前系统所处的安全级别，得出低、中、高的结论，包括所监视的网络设备的简要评价。

(2) 对偶然的、有经验的和专家级的黑客入侵系统做出时间上的评估和判断。

(3) 简要总结并给出重要的建议。

(4) 详细列举安全审计过程中的步骤，此时可以提出一些在侦查、渗透和控制阶段发现的问题。

(5) 对各种网络元素提出建议，包括路由器、端口、服务、登录账户、物理安全等。

(6) 讨论物理安全：许多网络对重要设备的摆放都不注意，例如有的公司把文件服务器置于接待台的桌子上，一旦接待人员离开，则服务器暴露在网络攻击下。

(7) 安全审计领域内使用的术语的介绍。

审计报告的内容根据审计任务的不同而有所区别。因此审计报告的内容及所附资料，要根据审计任务而定。一般从格式上来说，审计报告应包含审计任务与审计范围的说明、审计结论的提出及说明、建议事项及附件等模块。

审计报告是表达“审计目标、主要审计准则内容、审计范围、审计结果及结论的工具”。撰写报告时，审计人员需要积极与管理者及审计委员会沟通审计结果，撰写的报告应该客观、清晰、简洁、及时和有建设性，同时报告的表述应具有逻辑性，并且条理清楚，内容充足，并且要注意报告的及时发布，以保证迅速采取正确的措施。在报告最后发布之前，信息系统审计师应注意到组织或者环境的重大改变，做好后期事项。如果所发生的变化会影响到信息系统审计的发现与结论，信息系统审计师有责任采取恰当的措施，将这些改变及其潜在影响告知报告的收件人。这里所提及的重大改变往往包括发现应用系统控制中有欺骗行为，火灾等自然灾害，对软件系统生命周期各阶段的评审中发现的重大问题而导致项目延期或

终止，主要客户或供应商出现问题或者产品出现问题，参与项目实施的员工离职等。

7.7 信息风险事件的实时响应

2007年4月22日至27日，国际标准化组织技术管理局风险管理工作组（ISO/TMB/WG Risk Management）在加拿大渥太华召开了第四次工作组会议，会议将“风险”定义为不确定性目标的影响（The effect of uncertainty on objectives）。该定义克服了其他国家对“风险”定义过于狭窄、不准确的弊端，直指风险的本质，准确、全面、易于理解、便于应用。

“智者千虑，必有一失”。尽管已经开发了很多技术来保证信息系统的安全可靠运行，但要做到没有一点安全漏洞存在是很难的，更何况现在网络中各种入侵手段及入侵高手云集，系统受到入侵就会面临严重的灾难。这些影响信息系统安全的不当行为统称为风险事件。风险事件响应就是风险事件发生以后所采取的措施和行动。入侵技术的不断进化，再加上信息系统本身的脆弱性，使得入侵不可避免。因此，信息风险事件响应就成为一个与防火墙技术、入侵检测技术等同样重要的安全保障策略和手段。

安全是相对的，而风险却是绝对的。在制定风险事件的实时响应措施之前，必须先识别风险事件。一般认为，信息系统风险是系统的脆弱性和漏洞，以及以系统为目标的安全威胁和攻击的总称。系统脆弱性和漏洞是风险产生的原因，威胁和攻击是风险的结果。

信息系统中存在很多风险，但不是所有风险都会发生，它需要一定的发生条件，例如开放了Web服务器、网页遭到攻击者篡改等。这种安全风险事件的发生就可能是在一定条件下才有的，如没有及时响应，就会造成风险事故。

对任何信息系统来说，都存在各种各样或大或小的弱点，绝对的安全是不存在的，同样地，“零风险”是不存在的，正所谓“安全是相对的，风险是绝对的”。风险是对信息系统弱点进行利用后产生的负面影响，包括这种影响的可能性和已经发生的影响。潜在威胁信息系统安全的风险事件的形式多种多样，比如入侵者试图（不管成功与否）获得对系统或其数据的未授权访问；意外的破坏或者拒绝服务；未授权地使用系统处理或者存储数据；在所有者不知情、未指示或未同意情况下改变系统硬件、固件和软件特征；物理损害（火灾、地震、水灾或电源损坏等）；人为事故（偶然或不经意的行为造成的破坏）；设备故障（系统级外围设备故障）；内、外部攻击（内部人员或外部黑客的有无目的的攻击）；数据误用（共享机密数据或数据被窃）；数据丢失（故意或非故意的以破坏方式丢失数据）；程序错误（计算错误、输入错误或缓冲区溢出）。

由于风险具有时间动态性和空间分布性，因此必须制定实时的响应计划和措施。实时响应就是针对信息系统发生的有关系统安全方面的风险事件进行实时响应与分析，提出解决方案和应急对策，来保证信息系统和网络免遭破坏。

计算机信息系统的实时响应是一门综合性的技术学科，技术要求较高，是对突发安全事件进行响应、处理、恢复、跟踪的方法及过程，几乎与计算机信息系统安全学科内所有技术有关，主要包括以下几个方面。

1. 阻断技术

主要有3种阻断方式：

(1) ICMP 不可达响应——通过向被攻击主机或攻击源发送 ICMP 端口或目的不可达报文来阻断攻击。

(2) TCP-RST 响应——也称阻断会话响应,通过阻断攻击者和受害者之间的 TCP 会话来阻断攻击。这种机制是目前使用最多的主动响应机制。

(3) 防火墙联动响应——当入侵检测系统检测到攻击事件后向防火墙发送规则,由防火墙阻断当前以及后续攻击。

2. 攻击抑制技术

在计算机网络应急响应手段中,一种及时主动的应急响应技术就是攻击抑制技术。对于已经发生的信息安全事件,必须立即采取攻击源隔离等有效措施,对其进行抑制,以防止不良后果的继续扩大。攻击抑制是指通过各种技术手段限制攻击的范围,或是在被保护的信息系统遭受攻击时,采取各种技术手段,有效减少破坏行为。

抑制的目的是限制事件造成影响的范围和程度。是在事件发生的第一时间对故障系统或区域实施有效隔离和处理,或根据所拥有的资源状况和事件等级,采用临时关闭受影响系统并将业务切换到备份系统等措施降低损失、避免事件扩散和对受害系统的持续性破坏。抑制一般分为物理抑制、网络抑制、主机抑制和应用抑制。

研究抑制技术有助于在发生突发安全事件时降低或解除攻击的影响,其水平的高低也决定了应急响应效率的高低。主要涉及事件优先级认定、完整性检测和域名切换等技术。

3. 紧急恢复技术

在发生灾难性网络安全事件后可以通过紧急恢复技术进行系统恢复、数据恢复和功能恢复等工作,保持系统为可用状态或维持最基本服务能力。传统方法是采用磁盘镜像或数据备份技术以提高系统的可靠性。主要包括系统攻击可容忍性、网络结构的冗余容错和动态切换、计算机网络系统恢复、计算机远程恢复、计算机网络自修复等方面的研究。

通过应急恢复可以在遭受攻击后实现网络结构修复和重组、主机和服务器的恢复、数据库数据的安全恢复、网络配置的动态备份和快速恢复、网络受损分析与评估。

典型的恢复技术包括漏洞修补、业务连续性保障和灾难恢复等。常用工具有 Networker、ADSM、NetBackup、ARCserver 等。

4. 取证技术

取证技术是指对存储在计算机系统或网络设备中潜在电子证据的识别、收集、保护、检查和分析以及法庭出示的过程,通常是对存储介质、日志的检查和分析。计算机取证包括物理证据获取和信息发现两个阶段。在应急响应中,收集黑客入侵的证据是一项非常重要的工作。取证技术不但可以为打击计算机与网络犯罪提供重要支撑手段,还可为司法鉴定提供强有力的证据。

(1) 物理证据获取技术。指在计算机犯罪现场寻找并发现相关原始记录的技术,是取证工作的基础。在获取物理证据时最重要的工作是保证获取的原始证据不受破坏。关键技术是无损备份和删除文件的恢复。

① 无损备份技术。直接在被攻击机器的磁盘上进行取证操作,可能会损坏原始数据,因此要用磁盘镜像复制的办法,将被攻击机器的磁盘原样复制一份,然后对复制的磁盘进行取证分析。常用工具有 SafeBack、Ghost 等。

② 删除文件的恢复技术。在目前使用的操作系统中,即使将存储在硬盘的数据进行了删除操作,并清空回收站,数据仍然保留在硬盘上,只要该文件的存储位置没有被重新写入数据,原来的数据就可以恢复出来。常用工具有 Easy Recovery、Recover My Files 等。

(2) 信息发现技术。是指对获得的原始数据(文件、日志等)进行分析,从中寻找可以用来证明或者反驳的证据。具体手段包括:

① 日志分析技术。通过日志分析可以获得某时段 CPU 负荷、用户使用习惯、IP 来源、恶意访问提示等重要信息。常用的工具有 NetTracker、Logsurfer、Netlog 和 Analog 等。

② 数据捕获分析技术。在发现网络攻击行为后,通过截获和分析入侵者终端发出或者被入侵主机发出的网络数据包,可获得攻击源的地址和攻击的类型方法。常用工具有 TcpDump、WinDump、SNORT 等。

③ 解密技术。越来越多的计算机犯罪者使用加密技术保存关键文件,隐藏自己进行攻击的记录和操作。为了取得最终的攻击证据,取证人员应能将已发现的文件内容进行解密。

信息系统风险事件应急响应技术是信息安全中较为前沿的一个研究领域。随着研究的深入,突破了原 PDRR 模型的设想,将"响应"和"恢复"两种安全机制有机地结合起来,成为一个较为完善的应急响应系统。综合利用上述实时响应技术,充分发挥管理与机制在其中的作用,并不断改进相关规则来构建一个更为理想、完善的应急响应系统。应急响应的过程如下:

(1) 攻击信息分析。由入侵检测模块发现网络攻击,用分析处理模块对收集到的攻击信息进行分析整理,根据预先设定的策略和事件处置规则,在对攻击的危害程度和紧急程度做出基本判断的基础上,形成初步处置方案,并将处置方案和攻击信息通报管理平台。

(2) 简单情况处置。依据情况处置方案,对简单的网络扫描或危害性不高的攻击,系统自动启动阻断或隔离模块进行处理,防止发生进一步的网络攻击行为。对危害程度较高的攻击行为,则在启动阻断或隔离模块的同时,将攻击行为引入蜜罐模块中,避免攻击者对真实系统造成危害,并由蜜罐系统记录攻击者的攻击操作,同时调用追踪模块对攻击源进行追踪调查,收集并确定攻击信息。

(3) 综合分析处理。管理员通过分析管理平台、蜜罐模块和追踪模块收集到的信息,对自动防护方案进行调整,并可采取进一步的措施,如通过取证模块对攻击现场进行取证,调用加固优化模块及时修补导致攻击的漏洞来防止类似事件的发生,调用应急恢复模块对已被破坏的系统进行各类恢复操作等。

(4) 防护规则更新。事件处理完毕后,由管理员对此次的攻击行为及采取的应急防护措施进行综合分析,进一步完善分析处理机制,设定更为合理的防护规则,确保应急防护系统可以对下一次同样的攻击采取更为有效、及时的防护措施。

7.8 本章小结

安全管理贯穿于信息系统安全需求分析、规划设计、建设运行以及安全维护等各个阶段之中,既包含行政手段,也包含技术措施。本章所述的安全管理的内容包括信息系统安全组织机构管理、系统安全人事管理、安全系统管理、信息系统灾难恢复和安全审计管理以及信

息系统风险事件的实时响应等。学习本章内容，掌握与安全管理有关的内容与方法，将安全管理与技术相结合，确保信息系统的安全、可靠运营。

7.9 习　　题

1. 简述信息系统的安全组织结构。
2. 关于人员安全管理方面你有什么很好的建议?
3. 信息系统运行的安全管理目标是什么?
4. 系统评价指标有哪些?
5. 什么是安全事件? 简述安全事件的生命周期及安全事件的分类。
6. 简述应急计划的内容，应急事件处理的基本流程。
7. 如何对数据进行分类? 分为哪几类?
8. 灾难备份的衡量指标是什么?
9. 灾难备份方案分为几级? 主要的灾难备份技术有什么?
10. 简述如何选择合适的灾难恢复方案。
11. 如何做成本效益分析?
12. 简述灾难恢复过程。
13. 安全审计的概念及其功能简介。
14. 安全关联的作用有哪些?
15. 简述贝叶斯推理的内容。
16. 风险事件的分类有哪些?

第 8 章　信息系统安全风险评估

从机构的角度来看，信息系统安全问题是一个综合管理的问题。风险管理是信息系统安全运行的必要保证，是运行维护体系中最重要的环节，而风险评估则是风险管理的基础。本章将详细介绍风险评估的概念和过程，并介绍一些风险评估的标准和方法。

8.1　信息系统安全风险评估基础

一个单位或机构为了实现业务目标建设了信息系统，由于信息系统本身的弱点，信息系统面临着威胁，导致安全事件发生，造成一定的损害后果。

8.1.1　与风险评估相关的概念

风险(Risk)：由于系统存在的脆弱性，人为或自然的威胁导致资产的丢失或损害潜在发生的可能性及其造成的影响，即特定威胁事件发生的可能性与后果的结合。它由安全事件发生的可能性及其造成的影响这两项指标来衡量。

残余风险(Residual Risk)：采取了安全措施，提高了信息系统安全保障能力后，仍然可能存在的风险。

资产(Asset)：指任何对组织有价值的事物，是机构直接赋予了价值因而需要保护的东西，它可能以多种形式存在，无形的与有形的、软件与硬件、文档与代码等。

威胁(Threat)：指可能对资产和组织造成损害的事故的潜在原因。威胁可以通过威胁主体、资源、动机、途径等多种属性来描述。无论对于多么安全的信息系统，威胁是客观存在的，它是安全风险评估的要素之一。例如，组织的网络系统可能受到来自计算机病毒和黑客攻击的威胁。

脆弱性(Vulnerability)：指资产或组织中能被威胁利诱造成安全问题的不足和弱点。脆弱性也常被称为脆弱点。脆弱点包括物理环境、机构、过程、人员、管理、配置、硬件、软件和信息等各种资产的脆弱性。例如，员工缺乏信息安全意识、使用简短易被猜测的口令、操作系统本身有安全漏洞等。

风险评估(Risk Assessment)：指对信息和信息处理设施的威胁、影响和脆弱性及三者发生的可能性的评估。

风险评估也称风险分析，是对各方面风险进行辨识和分析的过程，就是确认安全风险及其大小的过程，即利用适当的风险评估工具，包括定性和定量的方法，确定资产风险等级和优先控制顺序。

风险管理(Risk Management)：是指基于风险分析的安全管理方法。风险管理是一个过程，其首要目的是保护机构以及该机构完成其使命的能力。风险管理包括对风险的识别、评估、控制的持续循环过程，并且风险管理必须满足成本效益平衡的原则。ISO/IEC

13335、ISO/IEC 27001 和 ISO/IEC 21827 等标准中均把风险管理作为安全管理的一个主要内容来进行讨论。

ISO/IEC 27001 中将风险管理定义为可以接受的费用识别、控制、降低或消除可能影响信息系统的安全风险的过程，即是一系列识别、控制、降低或消除安全风险的活动，通过风险评估来识别风险大小，通过制定信息系统安全方针，采取适当的控制目标与控制方式对风险进行控制，使风险被避免、转移或降至一个可被接受的水平。

国际标准 ISO/IEC 13335《信息技术安全管理指南》给出了信息安全、信息安全风险清晰的概念模型，明确了信息和信息系统安全风险组成的四要素：信息系统资产、信息系统脆弱性、信息安全威胁、信息系统安全保护措施，揭示了信息安全风险产生的内因、外因及其相互辩证关系：信息系统本身的脆弱性和安全保护措施的漏洞、薄弱点就是产生安全风险的内因，对资产的威胁欲望动机及其实施能力就是产生安全风险的外在因素；并明确表达了相对信息和信息系统现有保护措施的安全风险就是信息和信息系统安全残余风险的概念，使得人们对信息和信息系统安全概念的认识又深化了一层。图 8.1 显示了风险评估要素之间的主要关系。

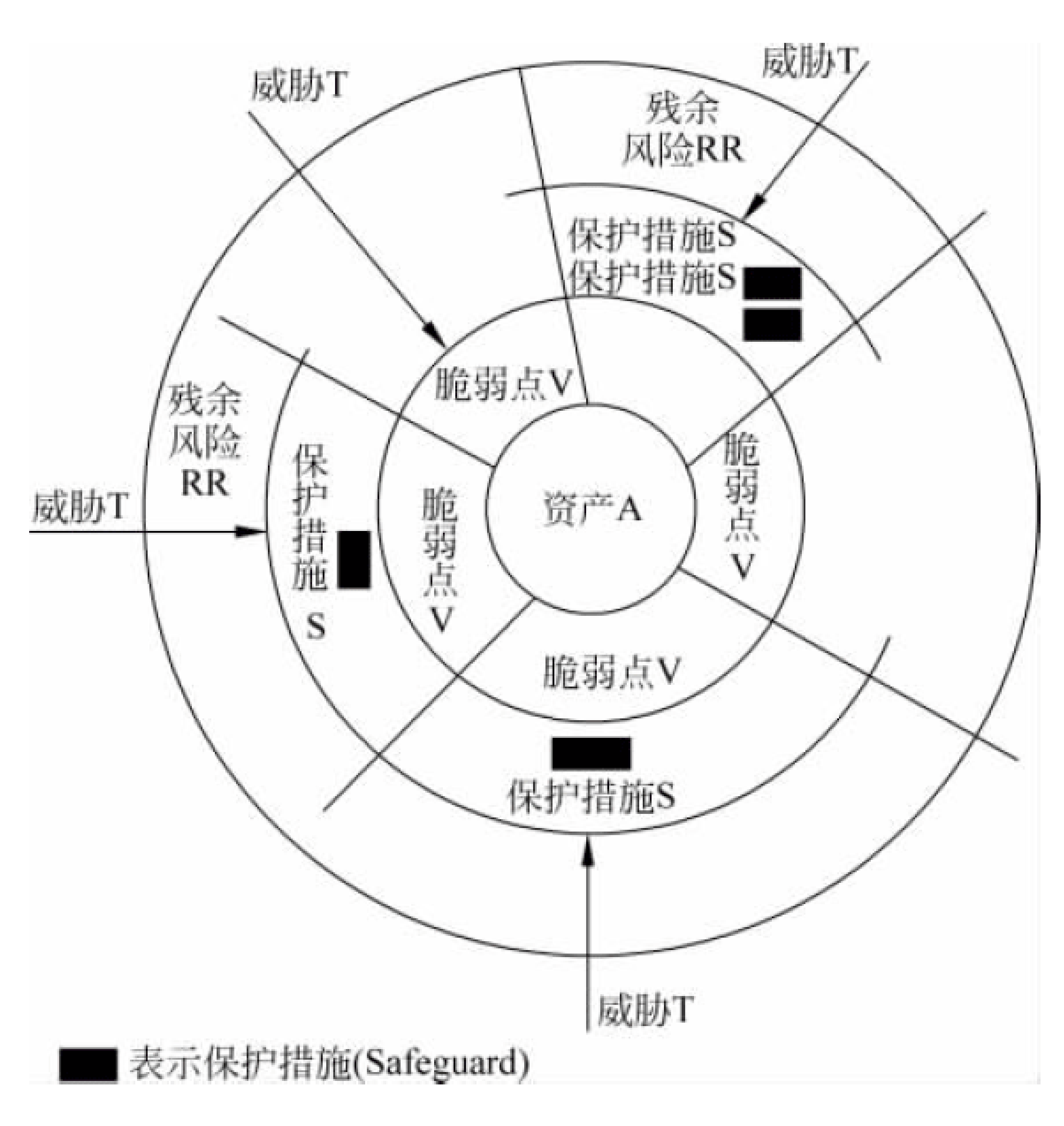


图 8.1　风险要素之间的主要关系

8.1.2　风险评估要素关系模型

信息系统安全风险评估要素包括资产、威胁、脆弱性和风险和安全措施。图 8.2 所给出的是信息系统安全风险评估的各要素的关系。其中，风险是核心，它的评估包括其他 3 个要素，即资产、威胁和脆弱性。信息系统安全风险评估过程中还需要充分考虑与基本要素密切相关的其他各类因素。

图 8.2 中方框部分的内容为风险评估的基本要素，椭圆部分的内容是与这些基本要素相关的属性。风险评估围绕着资产、威胁、脆弱性和安全措施这些基本要素展开，在对基本

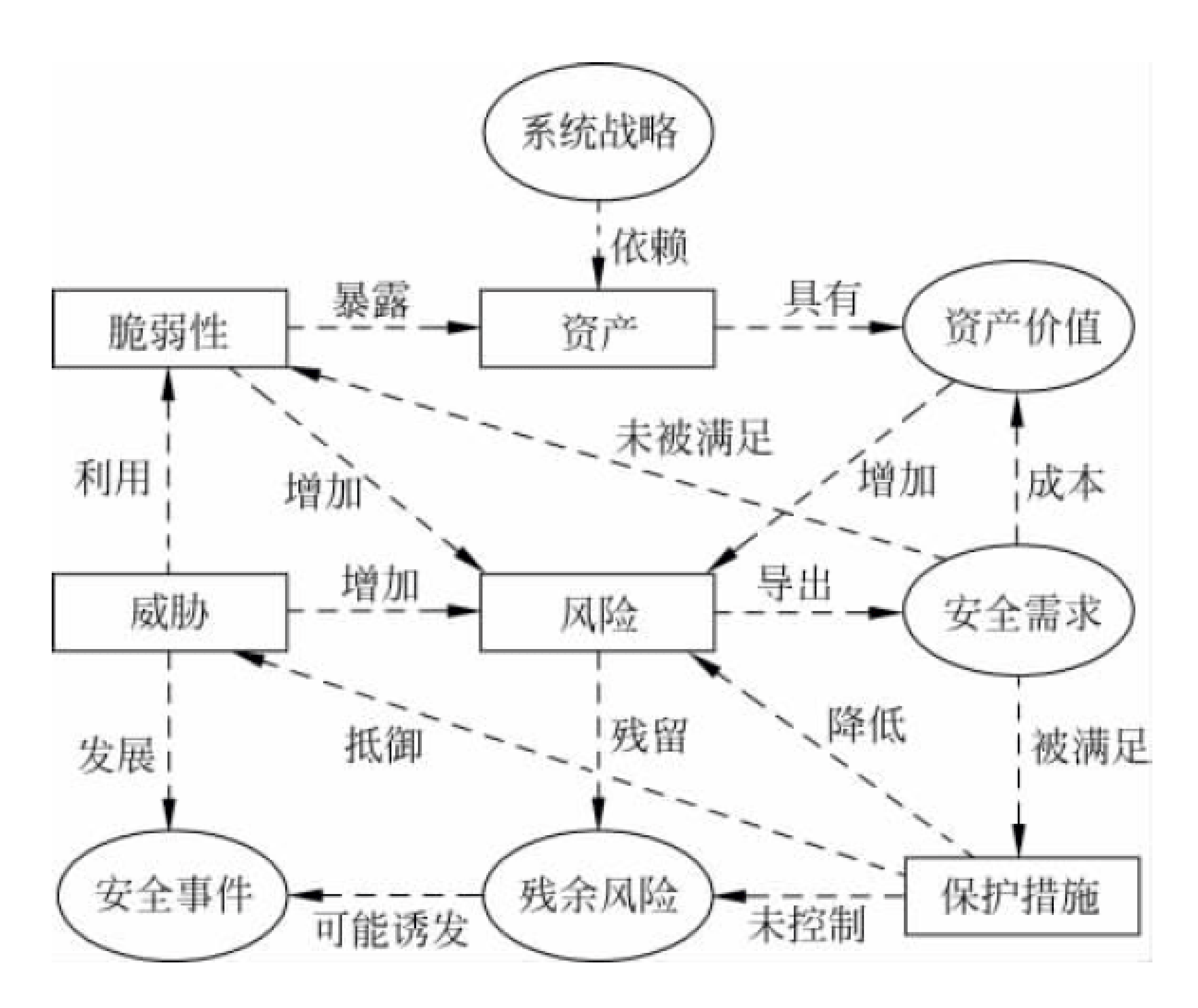


图 8.2　风险评估要素关系图

要素的评估过程中，需要充分考虑系统战略、资产价值、安全需求、安全事件、残余风险等与这些基本要素相关的各类属性。

图 8.2 中风险评估各要素和属性之间存在着以下关系。

(1) 系统战略的实现对资产具有依赖性，依赖程度越高，要求其风险越小。

(2) 资产是具有价值的，组织的系统战略越重要，对资产的依赖程度越高，资产价值就越大。

(3) 风险是由威胁引发的，资产面临的威胁越多则风险越大，并可能发展成为安全事件。

(4) 资产的脆弱性可能暴露资产的价值，威胁都要利用脆弱性，资产的脆弱性越多则风险越大。

(5) 脆弱性是未被满足的安全需求，威胁利用脆弱性危害资产，从而形成风险。

(6) 风险的存在及对风险的认识导出安全需求，安全需求可通过保护措施得以满足，需要结合资产价值考虑实施成本。

(7) 安全措施可抵御威胁，降低风险，减弱安全事件的影响。

(8) 风险不可能也没有必要降为零，在实施了安全措施后还会有残留下来的风险。有些残留风险是由于安全措施不当或无效，需要进行加强才可控制的风险，有些则是在综合考虑了安全成本与效益后不去有意控制的风险，这部分风险可以被接受。

(9) 残余风险应受到密切监视，它可能会在将来诱发新的安全事件的实施提供支持。

8.1.3　风险分析

风险分析原理如图 8.3 所示。

风险分析是风险评估的核心。风险分析中涉及资产、威胁、脆弱性 3 个基本要素。每个要素有各自的属性，资产的属性是资产价值；威胁的属性可以是威胁主体、影响对象、出现频率、动机等；脆弱性的属性是资产弱点的严重程度。

风险分析主要包括以下内容：

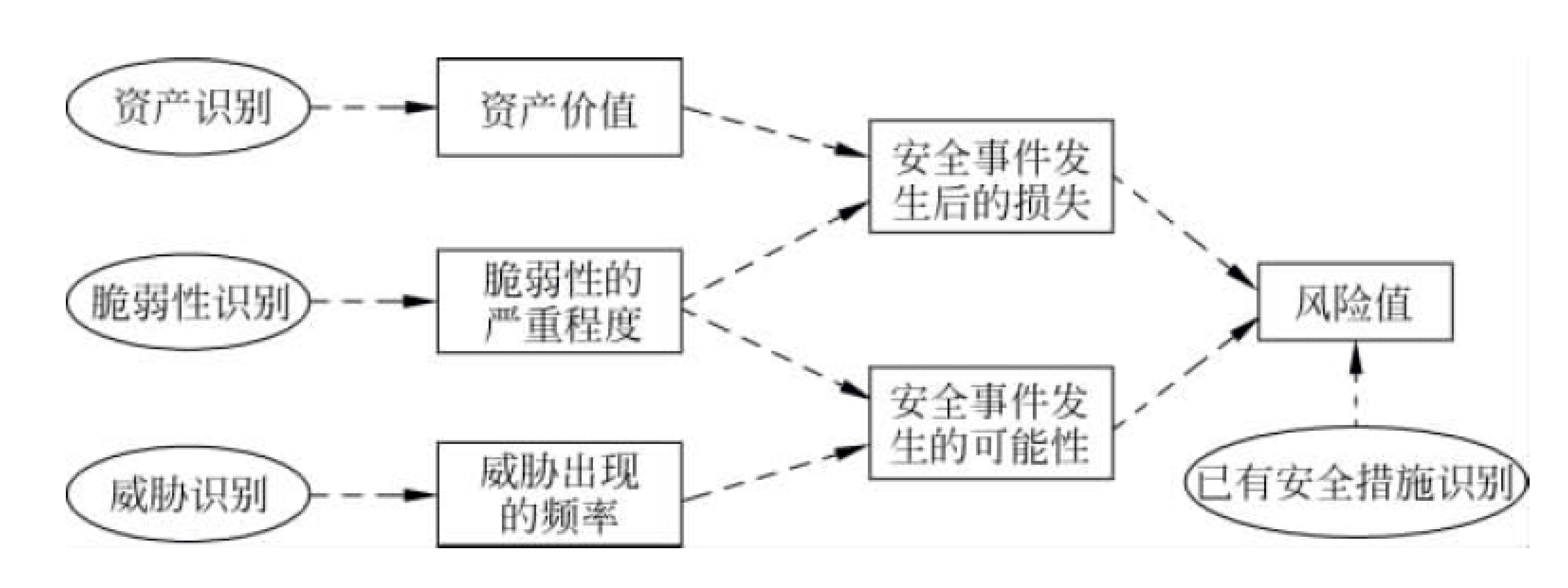


图 8.3　风险分析原理

(1) 对资产进行识别,并对资产的价值进行赋值。

(2) 对威胁进行识别,描述威胁的属性,并对威胁出现的频率赋值。

(3) 对脆弱性进行识别,并对具体资产的脆弱性的严重程度赋值。

(4) 根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性。

(5) 根据脆弱性的严重程度及安全事件所作用的资产的价值计算安全事件造成的损失。

(6) 根据安全事件发生的可能性以及安全事件出现后的损失,计算安全事件发生对组织的影响,即风险值。

8.1.4　信息系统安全风险评估的意义

通过风险评估,能及早发现问题并解决问题,防患于未然。当前,我国信息化发展过程中形成的基础信息网络和关系国家安全等方面的重要信息系统迫切需要进行持续的风险评估。通过风险评估可以有助于认清信息系统安全环境和信息系统安全状况,明确信息化建设中各级的责任,采取更加有效的安全保障措施,保证信息系统安全策略的一致性和持续性,进而为国家信息化发展服务,促进信息系统安全保障体系的建设,全面提高信息系统安全保障能力。风险评估的意义主要体现如下几个方面。

1. 加强风险评估工作是信息系统安全工作的客观需要

信息系统安全的实现是一个不断变化的过程,贯穿于信息系统建设的整个生命周期。信息系统安全的威胁可能来自内外部攻击造成的破坏,也可能来自信息系统本身所发生的意外事故。必须按照风险管理的思想,适时开展风险评估工作,妥善应对可能发生的问题。

2. 风险评估是信息系统安全建设和管理的关键环节

所有信息系统的安全建设和管理都应以风险评估为基础,只有全面正确地了解和掌握系统安全风险后,才能在控制风险、转移风险和减小风险之间做出正确判断,决定调用多少资源、以多大的代价、采取什么样的措施去控制风险。

3. 风险评估是需求主导和突出重点原则的具体体现

风险是客观存在的,完全避免风险或完全消灭风险是不现实的。要根据信息及信息系统的价值、威胁程度以及可能出现的问题的严重程度,科学地评估风险,并有效地控制风险。

4. 风险评估是分析确定风险的过程

系统的安全性可以通过风险大小来衡量。科学地分析系统的安全风险,综合平衡风险

和代价是风险评估的基本过程。风险评估是风险评估理论和方法在加强信息系统安全中的运用，是科学地分析信息系统在机密性、完整性和可用性等方面所面临的风险，通过采取安全措施减少风险，确保风险控制在可接受的范围内。

8.1.5 信息系统安全风险评估的内涵

1. 信息系统安全风险评估是信息系统安全建设和管理的科学方法

信息系统安全风险评估是保障信息系统安全的重要方法，它是风险管理理论和方法在信息化中的运用。信息系统安全风险评估是信息系统安全等级保护管理的工作，也是系统安全风险管理的重要环节。风险评估正确确定信息资产、合理分析信息系统安全风险、科学管理风险和控制风险。

信息系统安全的目的是保护信息资产免受威胁，但绝对安全可靠的网络系统并不存在，只能通过一定的措施把风险降低到可以接受的程度。信息系统安全评估是有效保证信息系统安全的前提条件，也是制定安全管理措施的重要依据。只有准确了解系统安全需求、安全漏洞及其可能的危害，才能制定并实施正确的安全策略。

风险评估通过一系列的技术和管理手段检测信息系统所处的安全级别、安全问题和安全漏洞，评估运行系统的风险，根据审计报告，制定适当的安全策略和实施规范，为安全体系的设计提供参考。

2. 信息系统安全风险评估是分析确定风险的过程

信息系统安全风险评估依据国家标准规范，对信息系统的机密性、完整性和可用性等安全保障性能进行综合评估活动。它利用适当的风险评估工具，确认信息资产自身的风险等级和风险控制的优先顺序，即确认安全风险及其大小的过程。风险评估是这样的过程，它识别系统安全风险，并确定风险出现的概率和结果造成的影响，提出补充的安全措施以缓和风险影响。风险评估是风险管理的组成部分。

3. 信息系统安全风险评估是信息系统安全建设的起点和基础

信息系统安全风险评估科学地分析理解信息及信息系统在机密性、完整性和可用性等方面所面临的风险，并做出决策，确定是预防风险、减少风险、转移风险还是补偿和分散风险等。风险评估分析现有系统的安全性，为降低系统安全风险、实施风险管理及风险控制提供直接依据。

信息系统安全建设的基本原则是从实际出发，坚持需求主导、突出重点。风险评估在实际工作中具体体现了这一原则。

4. 信息系统安全风险评估倡导适度安全

随着信息技术在国家各个领域的广泛应用，传统的安全管理方法已不能科学全面地分析、判断网络和信息系统的安全状态，在信息系统建设和运行过程中，出现了不能达到适当安全目标的偏差。

信息系统安全风险评估从风险管理的角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及存在的脆弱性，评估安全事件发生可能造成的危害程度，提出针对性抵御的防护对策和整改措施，并为防范信息系统安全风险，最大限度地保障信息系统安全提供科学依据，将风险控制在可接受的范围内。

风险评估在信息系统安全保障体系建设中具有不可替代的重要作用，它是实施等级保护的前提，也是检查、衡量系统安全状况的基础。

8.2 风险评估标准

经过多年风险评估研究与探索，国外发达国家初步建立了信息安全评估认证体系，陆续发布了一系列相关的标准、指南和规范，从标准、过程、方法与实践等方面都在一定程度上指导了各国的信息系统安全评估实践活动。目前国内外有关信息安全评估的标准有很多，本节将逐一进行介绍。

8.2.1 GB/T 20984-2007

国内标准主要是《信息安全风险评估规范》(GB/T 20984-2007)。2006 年 3 月 7 日国务院信息化办公室印发了由国家信息中心主持编写的《信息安全风险评估规范》(报批稿)，2007 年 7 月，该标准通过了国家标准化管理委员会的审查批准，标准编号与名称为 GB/T 20984-2007《信息安全技术 信息安全风险评估规范》于 2007 年 11 月正式实施。

该标准提出了风险评估的要素、实施流程、评估内容、评估方法及其在信息系统生命周期不同阶段的实施要点，适用于组织开展风险评估工作。

8.2.2 CC 标准

ISO/IEC 15408《信息技术安全性评估通用准则》(Common Criteria of Information Technical Security Evaluation，CCITSE)，简称 CC 标准，是由加拿大、美国及欧洲四国(共 6 国 7 个组织)经协商统一的准则，起草于 1993 年 6 月，国际标准化组织于 1999 年 6 月正式发布为国际标准，是目前最全面的评估准则。CC 2.0 版于 1999 年成为国际标准 ISO/IEC 15408，我国于 2001 年等同采用 GB/T 18336。ISO/IEC 15408 面向整个信息产品生存期，不仅考虑了保密性，而且还考虑了完整性和可用性等多方面的安全特性，侧重于对产品的技术指标的评估。

8.2.3 AS/NZS 4360

AS/NZS 4360：1999《风险管理标准》是澳大利亚和新西兰关于风险管理的标准，1995 年发行第一版，它是为满足公共和私人机构的高层管理者实际工作需要而产生的。AS/NZS 4360 提供的方法已经被澳大利亚政府和一些大的公众企业及英国国家卫生机构所采用，它为业界提供了风险管理方面的过程标准，即信息安全风险管理分为建立环境、风险识别、风险分析、风险评估和风险处理这 5 个标准环节。

8.2.4 BS 7799

BS 7799 标准是英国标准协会(BSI)制定的信息安全管理标准，是国际上具有代表性的信息安全管理体系标准，标准包括两部分：BS 7799-1：1999《信息安全管理实施准则》和 BS 7799-2：2002《信息安全管理体系规范》。标准的第一部分为第二部分的具体实施提供了指

南。BS 7799-1：1999《信息安全管理实施准则》是机构建立并实施信息安全管理体系的一个指导性准则，主要为机构制定信息安全策略和进行有效的信息安全控制提供一个通用的方案，BS 7799-1：1999 于 2000 年 12 月通过 ISO 认可，正式成为国际标准，即 ISO/IEC 17799：2000。BS 7799-2：2002《信息安全管理体系规范》规定了建立、实施和文件化信息安全管理系统(ISMS)的要求，规定了根据机构需要实施安全控制的要求，详细说明了建立、实施和维护信息安全管理系统的要求，提出了应如何建立信息安全管理体系的步骤。BS 7799-2：2002 已更新并在 2005 年 10 月正式发布为 ISO/IEC 27001：2005。BS 7799 标准要求各组织建立并运行一套经过验证的信息安全管理体系，用于解决资产的保管、组织的风险管理、安全措施选择、要求达到的安全程度等问题。根据 BS 7799 对信息安全管理框架和风险控制点的要求，可以设计完善的信息安全管理框架和风险管理体系。

8.2.5 ISO/IEC 13335

国际标准化组织发布的《信息技术安全管理指南》(ISO/IEC 13335)分为 5 个部分：

(1) ISO/IEC 13335-1：1996《信息安全的概念和模型》。

(2) ISO/IEC 13335-2：1997《信息安全管理与规划》。

(3) ISO/IEC 13335-3：1998《信息安全管理技术》。

(4) ISO/IEC 13335-4：2000《防护措施的选择》。

(5) ISO/IEC 13335-5：2001《网络安全管理指南》。

ISO/IEC 13335 首次给出了关于 IT 安全的机密性、完整性、可用性、审计性、认证性和可靠性 6 个方面定义，并提出了以风险为核心的安全模型，阐述了信息安全评估的思路，对信息安全评估工作具有指导意义。相比 BS 7799，它对安全管理的过程描述得更加细致。

8.2.6 NIST SP800-30

NIST SP800-30《IT 系统风险管理指南》，由 NIST 于 2002 年 1 月发布。NIST SP800-30《IT 系统风险管理指南》步骤清晰，描述流畅，对分级的定义言简意赅，基本采取三级定义法，比较适合初步开展风险评估的组织使用。NIST SP800-30《IT 系统风险管理指南》对自动化的信息系统处理信息及其使命完成，起到了重要的保护和支持作用。其中，风险管理共分风险评估、风险降低、在评估及评估 3 个过程。其中风险评估共分系统描述、脆弱性识别、威胁识别、控制分析、可能性判定、影响分析、风险判定、控制建议和结果文档 9 个步骤。此份指南的特点是风险评估结合信息系统生命周期的各个阶段而进行。

8.2.7 OCTAVE 标准

OCTAVE 是一种信息安全风险管理的方式。OCTAVE 标准是原则、属性和输出的集合，是适合组织自主进行的、综合的、系统的、与环境相关的信息安全风险评估方法。由此标准而产生的方法是灵活多变的，大部分被组织裁剪后都可以使用。此标准包括两种具体方法：OCTAVE 方法和 OCTAVE-S 方法。OCTAVE 方法主要是面向大型组织，而 OCTAVE-S 方法主要面向小型组织。在实际使用时，一个组织可能需要混合使用两种方法，或与 OCTAVE 完全不同的评估方式混合。

8.3　风险评估的两种方式

信息系统安全风险评估是提高我国信息系统安全保障水平的一项重要措施，应当贯穿于网络与信息系统建设运行的全过程。根据评估发起者的不同，风险评估可分为自评估和检查评估两种工作形式。信息系统安全风险评估应以自评估为主，自评估和检查评估相互结合、互为补充。

美国等发达国家的自评估工作已经实行多年，逐步形成了标准和规范，大体进入了制度化阶段。在此基础上，它们开始强调联邦级的认证认可及检查评估。我国开展信息系统安全风险评估工作滞后于发达国家。因此，现阶段应该把自评估工作尽快开展、规范起来，打好风险评估工作的基础。

8.3.1　自评估

自评估是指信息系统拥有、运营或使用单位发起的对本单位信息系统进行的风险评估，目的是发现信息系统现有的弱点。自评估是风险评估的基础，应结合系统特定的安全要求进行实施。根据“谁主管谁负责，谁运营谁负责”的原则，信息系统资产的拥有者、主管者、运行者首先应通过自评估的方式对自己负责，这样才能随时掌握安全状况，不断调整安全措施，有效进行安全控制。周期性进行的自评估可以在评估流程上适当简化，重点针对自上次评估后系统发生变化后引入的新威胁，以及系统脆弱性的完整识别，以便于两次评估结果的对比。

自评估是信息系统拥有者依靠自身力量，根据国家风险评估的管理规范和技术标准，对自有的信息系统进行风险评估的活动。信息系统的风险来自信息系统技术平台的共性和特定的应用服务。由于具体单位的信息系统特点不同，只有长期接触该单位所属行业和部门的人可以在短期内熟悉和掌握，而且只有拥有者对威胁及其后果的体会最深。信息技术企业通过技术平台的脆弱性分析，难以真正掌握和了解具体行业或部门的资产、威胁和风险。这些企业需要深入研究信息技术平台的共性化风险和推动不同行业部门的个性化风险的专门研究，否则风险评估的关注面将会缺失。

自评估可由发起方实施，也可以委托风险评估服务技术支持方实施。发起方实施的评估可以降低风险评估的费用、提高信息系统相关人员的安全意识，但可能缺乏风险评估的专业技能，造成结果不够深入准确；评估受到组织内部各种因素的影响，影响其结果的客观性。委托风险评估服务技术支持方实施的评估，过程比较规范、评估结果的客观性比较好，可信程度较高，但受到行业知识技能及业务了解的限制，对被评估系统的了解存在一定的局限性，尤其是在业务方面的特殊要求。另外，引入第三方本身就是一个风险因素，因此，应对第三方背景与资质、评估过程与结果的保密要求等方面进行控制。

此外，与系统相连的相关方也应配合工作，保证风险评估的实施，防止给其他方的使用带来困难和引入新的风险。

自评估方式的优缺点总结如下：

（1）优点——有利于降低风险评估的费用；有利于发挥行业和部门内的人员的业务特

长；有利于保密；有利于提高本单位的风险评估能力与信息系统安全知识。

(2) 缺点——在缺乏信息系统安全风险评估专业人才的情况下，如果没有统一的规范和要求，自评估的结果可能不深入和不规范；自评估中可能会存在某些不利的干预，影响风险评估结果的客观性，降低评估结果的置信度；某些时候，自评估的结果需要与管理层进行沟通。

为了尽量利用自评估的优点，降低缺点的影响，可以对自评估进行改进。例如，可以发挥专家的指导作用或委托专业评估组织参与部分工作，也可以委托具有相应资质的第三方机构提供技术支持。另外，由国家建立测评认证机构或安全企业实施评估活动，这样综合了自评估和第三方评估的优点。

委托第三方机构或组织参与自评估活动时，接受委托的评估机构拥有风险评估的专业人才，并且风险评估的经验比较丰富，对信息技术风险的共性了解得比较深入。另外，评估过程也较为规范，评估结果也比较客观，置信度比较高。但在委托第三方机构或组织参与自评估活动时需要注意，第三方机构可能会难以深入了解行业应用服务中的安全风险，并且风险评估中必然会接触到被评估单位的敏感信息，评估结果也属于敏感信息，委托评估中容易发生评估风险。另外，评估费用可能会很高。

8.3.2 检查评估

检查评估是指信息系统上级管理部门或国家有关信息系统安全职能部门依法组织的信息系统安全风险评估，目的是实施安全管理，检查被评估单位是否满足了这些标准或法规。检查评估是通过行政手段加强信息系统安全的重要措施。

检查评估的形式有安全保密检查、生产安全检查和专项检查。被查单位应配合评估工作的开展。

检查评估的实施可以依据国家标准或法规的要求，实施完整的风险评估过程，也可以在分析自评估过程的基础上，对关键环节或重点内容实施抽样评估。

检查评估的内容包括如下方面，但不仅限于此：

(1) 自评估队伍及技术人员检查。

(2) 自评估方法的检查。

(3) 自评估过程控制与文档记录的检查。

(4) 自评估资产列表审查。

(5) 自评估威胁列表审查。

(6) 自评估脆弱性列表审查。

(7) 现有安全措施有效性检查。

(8) 自评估结果审查与采取安全措施的跟踪检查。

(9) 自评估技术技能限制未完成项目的检查评估。

(10) 系统输入输出控制的检查。

(11) 上级关注或要求的关键环节和重点内容的检查评估。

(12) 软硬件维护制度及实施状况的检查。

(13) 突发事件应对措施的检查。

(14) 数据完整性保护措施的检查。

(15) 审计追踪的检查。

检查评估的模式是定期进行抽样,以检查关键领域或关键点的信息系统安全风险是否在可接受的范围内。在检查评估实施之前,一般应确定适用于整个评估工作的评估要求或规范,以适用于所有被评估单位。

检查评估一般是由被评估方的主管机构实施的,被检查单位自身不能对评估过程进行干预,所以其评估结果最具权威性。

检查评估本身也有一定的限制,例如评估间隔时间较长,有时还是抽样进行;评估不能贯穿整个部门信息系统生命周期的全过程,很难对信息系统的整体风险状况做出完整的评价。

检查评估也可以委托风险评估服务技术支持方实施,但评估结果仅对检查评估的发起组织负责。由于检查评估代表了主管机构,涉及评估对象也往往较多,需要对实施检查评估的机构的资质进行严格管理。

8.4　风险评估的过程

信息系统安全风险评估是依据有关信息安全技术与管理标准,对信息在产生、存储和传输等过程中其机密性、完整性和可用性等安全属性进行评价,评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性,并结合安全事件所涉及的资产价值来判断安全事件发生对组织造成的影响。无论选择哪种风险评估方法,都会涉及以下基本要素:

(1) 识别要评估的资产。

(2) 确定资产的威胁、脆弱性及相关问题。

(3) 识别风险的高低次序。

(4) 完成控制措施或接受风险。

(5) 监督控制措施的有效性或评估其有效性。

8.4.1　风险评估基本流程

风险评估的基本流程如图 8.4 所示。

首先是风险评估的准备阶段,进行组织准备、技术准备、人员准备和资金准备。然后是风险评估要素的识别和赋值,包括以下内容:

(1) 对信息资产进行识别,并对资产赋值。

(2) 对威胁进行识别,并对威胁发生的可能性赋值。

(3) 对信息资产的脆弱性进行识别,并对脆弱性的严重程度赋值。

(4) 根据威胁和脆弱性计算安全事件发生的可能性。

(5) 结合信息资产的重要性和在此资产上发生安全事件的可能性计算信息资产的风险值。

最后是记录风险评估的结果。

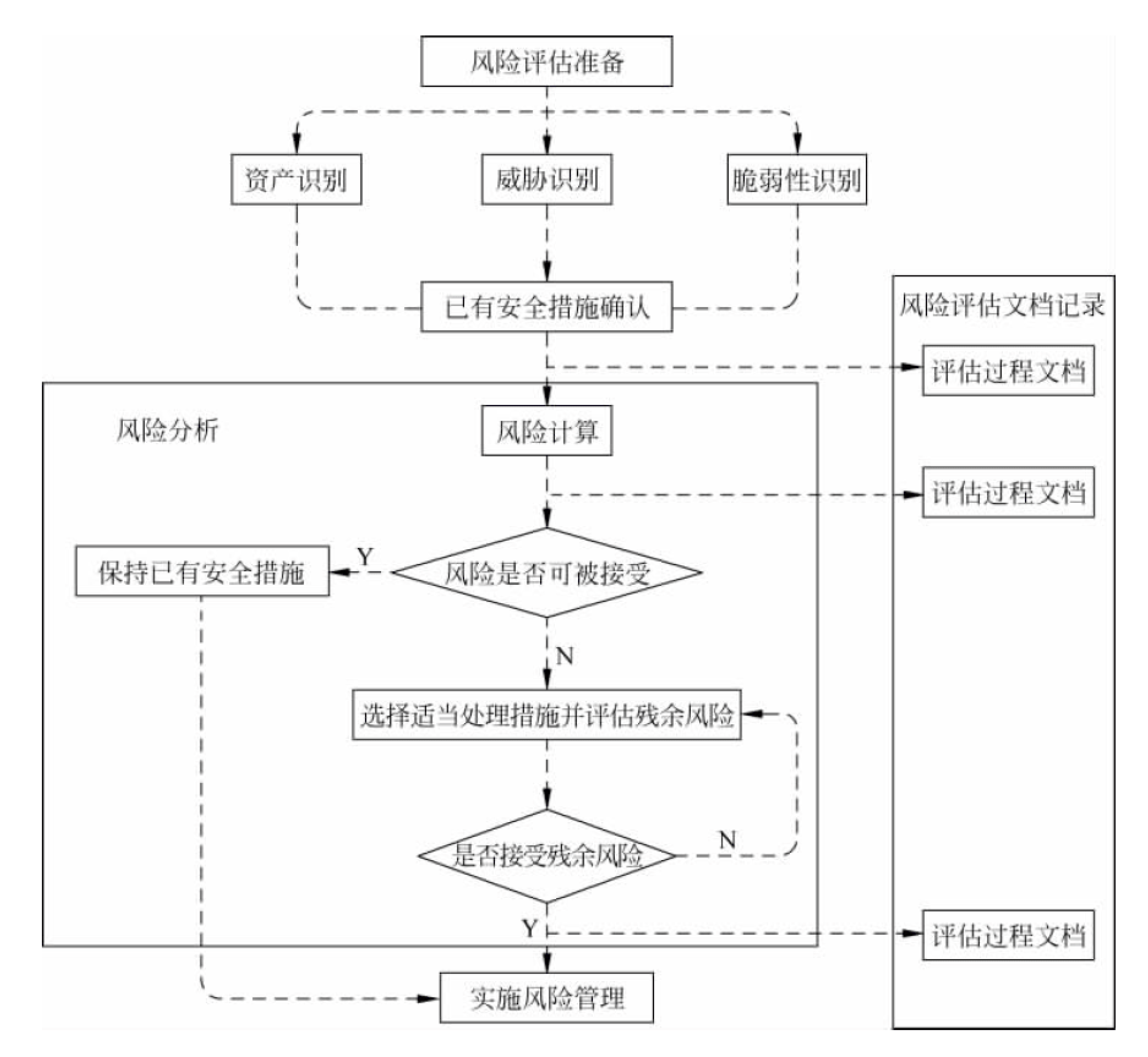


图 8.4 信息系统安全风险评估基本流程

8.4.2 风险评估准备

风险评估的准备过程是组织进行风险评估的基础，是使整个风险评估过程高效完成的保证。组织对自身信息系统计划实施风险评估是一种战略性考虑，其结果将受到组织业务需求、战略目标、业务流程、安全需求、系统规模和组织结构等方面的影响。不同的组织对风险评估的实施过程可能存在不同的要求。因此，在实施风险评估之前，应做到以下几点：

(1) 确定风险评估的目标。

(2) 确定风险评估的范围。

(3) 确定组织的结构。

(4) 进行系统调研。

(5) 选择风险评估方法和工具。

(6) 获得最高管理者的支持。

1. 确定风险评估的目标

在风险评估准备阶段应明确风险评估的目标，为风险评估的过程提供导向。支持组织业务战略的信息、系统、应用软件和网络是组织的重要资产，其机密性、可用性和完整性对维持企业的竞争优势、获利能力、法规要求和企业形象等具有十分重要的意义。风险评估目标

需满足企业持续发展在安全方面的要求，满足相关方的要求，满足法律法规的要求等。组织进行信息系统安全风险评估活动的需求是实际存在的，无论出于何种动机，风险评估的目标可大致总结如下：

1）了解安全现状

对信息资产的识别，明确了组织的保护对象及保护对象的优先级序列；威胁识别明确了组织所面临的安全威胁，这些威胁可能来自于组织的内部和外部；脆弱性识别可以使组织得到当前信息系统漏洞的统计及分布情况；安全控制措施的识别和确认可以清晰地描述出当前的安全体系的安全控制措施；风险分析则将上述要素进行关联分析，从组织业务和战略的角度去描述和量化组织的安全风险。

2）辅助管理层决策

组织的管理人员都希望能够将有效的资金和人力投入到信息系统安全最迫切需要的环节，以获得最大化的安全收益，而且收益是可验证的。信息系统安全风险评估活动可以帮助组织实现这种愿望。在风险评估识别阶段完成后，风险的主要构成要素均已被识别。在风险分析阶段，经过对信息系统安全风险的描述、量化和展现，被评估组织管理层可以从组织业务和战略的高度，了解信息系统安全风险。

3）强制符合性检查

组织为了满足某些内部或外部的强制要求进行风险评估。内部要求通常是组织自身的信息系统安全策略或有关信息系统安全的规定；外部要求包括法律、强制性标准和行业规范等。随着信息化水平的逐步提高和信息系统安全问题日益突出，会有越来越多的有关信息系统安全的法律和标准推出，出于此类目的而进行风险评估的组织也会随之增加。

2. 确定风险评估的范围

任何一项评估工作开始之前，都应清楚地界定出评估的范围。在划定评估范围时，只有从组织的业务入手，才能把安全策略、组织和人员、安全管理和操作实践以及信息系统本身等风险评估需要考虑的各个方面有机地结合起来，也只有从业务层面入手，分析阶段中的分析工作，才会有实际意义。

组织进行风险评估可能是自身商业需求及战略目标的要求、相关方的要求或其他原因，应根据上述原因确定风险评估范围。范围可能是组织内部的信息和信息系统，可能是单独的信息系统，可能是组织的关键业务流程，也可能是客户的知识产权。描述范围时，最重要的是对于评估边界的描述，确定了清晰的评估边界，就相当于规定了对风险评估小组的授权范围，并且提供了进行评估的必要信息。

一旦确定了需要评估的业务范畴，评估活动就可以从以下方面确定相应的评估范围。

1）信息系统

业务系统选定后，支持该业务运转的信息系统也就随之确定。在风险评估的识别阶段，需要识别信息资产、威胁、脆弱性以及已有安全措施等重要信息，这些信息都直接或间接地来自于信息系统本身。在描述信息系统的评估范围时，为了避免重叠或遗漏，可以按照不同层次，对实体资产进行分类和列表。

2）组织结构和人员

被评估组织会有一定的组织结构和人员。“人”才是信息系统安全活动的主体，每个人承担着特定的业务职责。由人构成一个个部门，不同的部门构成层次化组织结构。信息系

统安全风险评估不再只是单纯的技术，评估活动会更加关注安全管理、整体安全、安全体系建设等方面。

3）安全管理和实践活动

安全管理和实践活动一般设在评估流程的安全措施的识别与确定环节。如果没有有效的管理和操作过程保障，再好的安全措施也无法发挥其作用。实际上，在信息系统的组织和人员的范围确定后，从主体和客体的角度也就确定了安全管理与操作的范围。

4）地理范围

业务范围确定后，评估活动要检查的地理范围相应地也就被确定了。如果是具有较大地域分布的大型组织，并且不同地点的业务具有很强的独立性，就需要在空间上明确哪些地点属于评估的范围。

3. 确定组织的结构

确定组织的结构即建立风险评估团队，以支持整个过程的顺利推进。风险评估团队的成员是指评估过程中的管理者以及具体评估活动的实施者。组织结构的确定应考虑其结构的复杂程度，以保证能够满足风险评估的范围和目标。风险评估团队应能够保证风险评估工作的高效进展。

在选择风险评估团队成员时，不仅要考虑技术部门，也要考虑各个部门的搭配，团队应包括以下成员：

（1）风险评估的专家级人物，或者即将成为专家级的人物。他们具有丰富的评估经验和专业知识，为评估工作提供后台技术支持。辅助高层决策，目的是持续地领导具体的风险工作。

（2）技术专家。技术漏洞虽然不是最重要的，但在风险评估的过程中技术漏洞却是最琐碎的。评估过程中要涉及很多的技术问题，所以需要技术专家为团队成员解释和指导专业问题。

（3）如果组织已经通过质量管理体系、环境管理体系等其他体系，团队需要相关体系的负责人员负责文档评估的问题。

对于风险评估团队的建立并没有准则而言，组织可以按照自身的情况来配备相关的人员。风险评估专家和技术专家一般是必需的。

4. 系统调研

系统调研是确定被评估对象的过程，风险评估团队应进行充分的系统调研，为确定风险评估目标、评估依据和方法的选择和评估内容的实施提供基础。调研内容至少应包括：

（1）业务战略及管理制度。

（2）主要的业务功能和要求。

（3）网络结构与网络环境，包括内部连接和外部连接。

（4）系统边界。

（5）主要的软件和硬件。

（6）数据和信息。

（7）系统和数据的敏感性。

（8）支持和使用系统的人员。

系统调研可以采取问卷调查、现场面谈相结合的方式进行。调查问卷是提供一套关于管理或操作控制的问题表格,供系统技术或管理人员填写。现场面谈是由评估人员到现场观察并收集系统在物理、环境和操作方面的信息。

5. 选择风险评估方法和工具

风险评估方法应考虑评估的范围、目标、时间、效果、组织文化、人员素质以及具体开展的程度等因素来确定,使之能够与组织的环境和安全要求相一致。

评估过程中需要用到风险评估工具,应根据需要进行选择。

6. 获得最高管理者对风险评估的支持

风险评估过程应得到组织最高管理者的支持、批准,并对管理层和技术人员进行传达,在组织内部对风险评估相关内容进行培训,以明确有关人员在风险评估中的任务。

8.4.3　资产识别

信息资产是具有价值的信息或资源,它能以多种形式存在,有无形的和有形的,有硬件和软件,有文档和代码,也有服务和形象等。对信息资产而言,主要包括 3 个部分:信息本身、信息处理设施和信息处理人员。广义上讲,组织内所有资产和信息都有联系,都可以作为信息资产而被识别。在实践过程中,信息处理设施往往属于固定资产的范畴,一般都已经得到良好的管理,而人员管理有专门的人力资源管理资料可用,且评估应该有其他的方法。

机密性、完整性和可用性是评价信息资产的 3 个安全属性。信息资产安全特性的不同也决定了其信息价值的不同,以及存在的弱点、面临的威胁、需要进行的保护和安全控制都各不相同。风险评估中资产的价值不仅仅以资产的经济价值来衡量,也由资产在 3 个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定。安全属性达成程度的不同将使资产具有不同的价值,而资产面临的威胁、存在的脆弱性以及已采用的安全措施都将对资产安全属性的达成程度产生影响。因此,有必要对组织中的资产进行识别。

资产识别的首先工作是对资产进行分类,然后对每项资产的机密性、完整性和可用性进行赋值,在此基础上评价资产的重要性。

1. 资产分类

在一般的评估体中,资产有多种表现形式,资产大多属于不同的信息系统,如办公自动化系统、网管系统、业务生产系统等。对于提供多种业务的组织,其支持业务持续运行的系统数量可能会很多。因此首先需要将信息系统及其相关的信息资产进行分类,才能在此基础上进行下一步的风险评估工作。在实际工作中,具体的资产分类方法可以根据具体评估对象、要求和具体环境,由评估者灵活把握。例如可以按用途分类,也可以按安全级别分类。

表 8.1 给出了一个信息资产分类示例。

表 8.1 信息资产分类示例

资产分类	资 产 示 例
数据	电子媒介数据，包括源代码、数据库数据、数据资料、系统文档、运行管理规程、计划、报告、产品信息等
硬件	计算机、打印机、路由器、交换机、硬件防火墙、程序交换机等
软件	应用程序、系统软件、开发工具、资源库等
文档	纸质的各种文件、传真、财务报告、发展计划等
服务	WWW、SMTP、POP3、FTP、网络连接、网络管理、入侵监控等信息服务
环境设备	电源、空调、文件柜、消防设施等
人员	各级雇员、雇主、合同方雇员等
其他	企业形象、客户关系等

2. 资产赋值

信息资产的赋值是进行风险评估的关键，如果参与风险评估的人员对信息资产的价值没有统一的认识，进行准确的风险评估则很困难。

资产赋值是对资产安全价值的估价，不仅要考虑资产的成本价格，更要考虑资产对于组织业务的安全重要性，即根据资产损失所引发的潜在影响来决定。对信息资产进行赋值并不是一件容易的事情，通常需要资产拥有者的积极配合。

资产赋值可以为机密性、可用性和完整性这 3 个安全特性分别赋予不同的价值等级，也可以用相对信息价值的货币来衡量。资产赋值的过程也就是对资产在机密性、完整性和可用性影响分析的过程。资产对机密性、完整性和可用性上的要求可由安全属性缺失时造成的影响来表示，这种影响有人为或突发性引起的安全事件对资产破坏的后果。这一后果可能毁灭某些资产，危及信息系统并使其丧失机密性、完整性和可用性，最终会导致财政损失、市场份额或公司形象的损失。

资产安全属性的不同，通常也意味着安全控制、保护功能需求的不同。通过考察 3 种不同的安全属性，基本能够了解资产的价值。

1）资产机密性赋值

根据资产在机密性方面的不同要求，将其分为不同的等级，分别对应资产在机密性方面的价值或者机密性受到损失时对整个组织的影响。表 8.2 列出了一种资产机密性赋值的参考。

表 8.2 资产机密性赋值

赋值	标识	定 义
1	可忽略	可对社会公开的信息、公用的信息处理设备和信息资源等信息资产
2	低	仅在组织内部或某一部门内部公开的信息，向外扩散有可能对组织的安全和利益造成轻微损害
3	中等	组织的一般性机密，其泄露会使组织的安全和利益受到损害
4	高	组织的重要秘密，其泄露会使组织的安全和利益遭受到严重损害
5	很高	组织最重要的机密，关系未来发展的前途命运，对组织根本利益有着决定性的影响，如果泄露会造成灾难性的损害

2）资产完整性赋值

根据资产在完整性方面的不同要求，将其分为不同的等级，分别对应资产在完整性方面的价值或者完整性受到损失时对整个组织的影响。表 8.3 列出了一种有关资产完整性赋值的参考。

表 8.3　资产完整性赋值

赋值	标识	定　义
1	可忽略	完整性价值非常低，未经授权的修改或破坏对组织造成的影响可以忽略，对业务冲击可以忽略
2	低	完整性价值较低，未经授权的修改或破坏会对组织造成轻微影响，可以忍受，对业务冲击轻微，损失容易弥补
3	中等	完整性价值中等，未经授权的修改或破坏会对组织造成影响，对业务冲击明显，但损失可以弥补
4	高	完整性价值较高，未经授权的修改或破坏会对组织造成重大影响，对业务冲击严重，损失比较难以弥补
5	很高	完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，对业务冲击重大并可能造成严重的业务中断，损失难以弥补

3）资产可用性赋值

根据资产在可用性方面的不同要求，将其分为不同的等级，分别对应资产在可用性方面的价值或者可用性受到损失时对整个组织的影响。表 8.4 提供了一种有关资产可用性赋值的参考。

表 8.4　资产可用性赋值

赋值	标识	定　义
1	可忽略	可用价值可以忽略，合法使用者对信息及信息系统资源的可用度在正常工作时间低于 25%
2	低	可用价值较低，合法使用者对信息及信息系统资源的可用度在正常工作时间达到 25%以上，或系统允许中断时间小于 60 分钟
3	中等	可用价值中等，合法使用者对信息及信息系统资源的可用度在正常工作时间达到 70%以上，或系统允许中断时间小于 30 分钟
4	高	可用价值较高，合法使用者对信息及信息系统资源的可用度达到每天 90%以上，或系统允许中断时间小于 10 分钟
5	很高	可用价值非常高，合法使用者对信息及信息系统资源的可用度达到年度 99.9%以上，或系统不允许中断

4）资产重要性等级

资产价值可以通过资产在机密性、完整性和可用性方面的赋值等级，经过综合评定得出资产价值。资产的赋值采用定性的相对等级方式。与安全属性的等级相对应，资产的等级可分为 5 级，从 1～5 由低到高分别代表 5 个级别的资产相对价值，等级越高表示资产的重要性程度越高。表 8.5 提供了一个有关资产重要性等级划分的参考，1～5 赋值方法。此外还有 1～3 赋值法和 1～9 赋值法等。

表 8.5 资产重要性等级

赋值	标识	定 义
1	可忽略	资产的重要程度很低，其安全属性遭到破坏后可能导致系统受到很低程度的影响，对组织造成的损失很小，可以忽略不计
2	低	资产的重要程度较低，其安全属性遭到破坏后可能导致系统受到较低程度的影响，对组织造成较低的损失
3	中等	资产的重要程度中等，其安全属性遭到破坏后可能导致系统受到中等程度的影响，对组织造成中等程度的损失
4	高	资产的重要程度较高，其安全属性遭到破坏后可能导致系统受到比较严重的影响，对组织造成比较严重的损失
5	很高	资产的重要程度很高，其安全属性遭到破坏后可能导致系统受到非常严重的影响，对组织造成非常严重的损失

由于资产最终价值的等级评估是依据资产机密性、完整性和可用性的赋值级别，经过综合评定得出的，评定准则可以根据组织自身的特点，选择对资产机密性、完整性和可用性最重要的一个属性赋值等级作为综合资产赋值准则，也可以根据资产机密性、完整性和可用性的综合评定作为准则。评估者也可以根据被评估系统的实际情况自定义资产的等级。这种方法可以作为等级保护中确定安全等级的参考。

8.4.4 威胁识别

威胁是可能导致对系统或组织及其资产造成破坏的潜在可能性因素。造成威胁的因素可分为环境因素和人为因素。环境因素包括自然界的不可抗因素和其他物理因素。人为因素根据威胁的动机可分为恶意和非恶意。威胁的作用形式可以是对组织信息直接或间接的攻击，如非授权的泄露、删除、篡改等，从而使信息资产在机密性、可用性或完整性等方面造成损害，也可能源自偶然或蓄意的事件。

一般来说，威胁只有利用系统、应用或服务的弱点才有可能对资产成功实施破坏。威胁被定义为不期望发生的事件，这些事件会影响业务的正常运行，使组织不能顺利达成其最终目标。一些威胁是在已存在控制措施的情况下发生的，这些控制措施可能是没有正确配置或超过有效期的，因此为威胁进入操作环境提供了机会，这个过程就是通常所说的利用漏洞的过程。安全事件及其后果是分析威胁的重要依据，但是有一部分威胁发生时，由于未对系统造成危害而被安全管理人员忽略，导致对安全威胁的认识出现偏差。

威胁发生的可能性受以下两方面因素影响：

(1) 资产的吸引力和曝光程度、组织的知名度，这主要在考虑人为故意威胁时使用。

(2) 资产转化为利润的容易程度，包括财务的利益、黑客的能力很强和带宽很大的主机的使用权等利益，这主要在考虑人为因素威胁时使用。

1. 威胁分类

在对威胁进行分类之前，应先考虑威胁的来源。表 8.6 列出了一系列威胁来源，此表只是一种威胁来源表，不能认为表 8.6 包含了全部的威胁来源。

表 8.6　威胁来源

威 胁 来 源		威胁来源描述
环境因素		断电、雷击、静电、灰尘、潮湿、温度、电磁干扰、火灾、水灾、地震、鼠蚁虫害、意外事故等环境危害或自然灾害，以及软硬件、数据、通信线路的故障等
人为因素	恶意内部人员	不满的或有预谋的内部人员对信息系统进行恶意破坏，采用自主或内外勾结的方式盗窃机密信息或篡改，获取利益
	非恶意内部人员	内部人员缺乏责任心，或者不关心和不专注，或者没有遵守规章制度和操作流程，导致故障或信息损坏，或内部人员缺乏培训、专业技能不足，不具备岗位技能要求而导致信息系统故障或被攻击
	第三方	合作伙伴或供应商，包括移动、电信、证券、税务等业务合作伙伴以及软件开发合作商、系统集成商、服务商和产品提供商，包括第三方恶意和非恶意行为
	外部攻击人员	外部人员利用信息系统的脆弱性，对网络或系统的机密性、完整性和可用性造成破坏，以获取利益或炫耀能力

列出了威胁来源之后，对威胁来源进行分类。分类的方式有多种，表 8.7 给出了一种威胁分类方法。

表 8.7　一种威胁分类表

威 胁 分 类	威胁分类描述
物理环境	断电、雷击、静电、灰尘、潮湿、温度、电磁干扰、火灾、水灾、地震、鼠蚁虫害、意外事故等对信息系统造成影响的物理环境或自然灾害
软硬件故障	由于设备硬件故障、通信线路中断、系统本身或软件缺陷，对系统运行造成影响
恶意代码和病毒	具有自我复制和传播能力，故意在系统上执行恶意程序的程序代码
物理攻击	物理接触、物理破坏或盗窃
网络攻击	通过黑客手段，如密码猜测、缓冲区溢出、安装后门、嗅探、拒绝服务等对信息系统进行攻击和入侵
无作为或操作失误	该执行而没有执行相应操作，或无意执行错误的操作对系统造成影响
管理缺陷	安全管理无法落实或不到位，管理不规范和混乱，造成信息系统造成影响
越权或滥用	访问无权访问的资源，或滥用权限，使信息系统受到破坏
泄密、篡改和抵赖	将机密信息泄露给他人，非法修改信息，破坏系统的机密性和完整性，不承认收到信息和所作的操作和交易

2. 威胁分析

在对威胁进行赋值之前，首先需要对威胁进行分析，威胁分析主要包括以下内容。

1）潜在威胁分析

潜在威胁分析是指对用户信息系统安全方面的潜在威胁和可能入侵做出全面的分析。潜在威胁主要是指根据资产的脆弱性而引发的安全威胁。通过对漏洞的进一步分析，可以对漏洞可能引发的威胁进行赋值，赋值主要依据威胁发生的可能性和造成后果的严重性。潜在威胁分析过程主要基于威胁列表和统计信息。

2）威胁审计和入侵检测

威胁审计和入侵检测是指利用审计和技术工具对组织面临的威胁进行分析。威胁审计是指利用审计手段发现组织曾经发生过的威胁并加以分析。威胁审计的对象主要包括组织的安全事件记录、故障记录、系统日志等。威胁审计的过程中包括：咨询顾问收集历史资

料；寻找异常现象；发现威胁情况并编写审计报告。入侵检测主要是指利用入侵检测系统对组织网络当前阶段所经受的内外部攻击或威胁进行分析。在入侵检测过程中，操作人员需编写检测方案，然后部署入侵检测系统，对来自内外部的攻击行为进行检测。入侵检测完成后，分析人员根据入侵检测系统的日志完成分析报告。

3）安全威胁综合分析

安全威胁综合分析是对前两项分析结果进行的综合分析，以便给出全面的威胁分析报告。威胁分析报告的内容与信息资产存在的漏洞相对应，并对威胁进行相应的赋值。

3. 威胁赋值

评估确定威胁发生的可能性是威胁评估阶段的重要工作，评估者应根据经验或统计数据来判断威胁发生的概率。威胁发生的可能性受以下因素影响。

(1) 资产的吸引力。

(2) 资产转化为报酬的难易程度。

(3) 威胁源的技术力量和所掌握的资源。

(4) 脆弱性被利用的难易程度。

(5) 入侵者的水平。

(6) 信息系统的管理水平。

在实际评估中，还需要综合考虑以下 3 个方面的内容，以确定在特定环境中各种威胁出现的频率。

(1) 过去安全事件报告或记录中出现过的威胁及其频率的统计。

(2) 实际评估环境中通过检测工具以及各种日志发现的威胁及其频率的统计。

(3) 过去一年来国际机构发布的对于整个社会和特定行业的安全威胁发生频率的统计以及威胁预警。

表 8.8 是一种威胁出现频率的赋值表。在实际评估中，威胁频率的判断依据应在评估准备阶段根据历史统计或行业判断予以确定，并得到被评估方的认可。

表 8.8 威胁赋值表

赋值	标识	威胁可能性定义
1	可忽略	威胁几乎不可能发生，仅可能在非常罕见的情况下发生
2	低	威胁发生的可能性较低，一般不可能发生，或没有被证实发生过
3	中等	威胁发生的可能性中等，至少半年发生一次，或在某种情况下可能会发生，但未被证实发生过
4	高	威胁发生的可能性较高，至少每月一次，或在大多数情况下都可能会发生，或可以证实多次发生过
5	很高	威胁发生的可能性很高，至少每周一次，或在大多数情况下几乎不可能避免，或者可以被证实经常发生

8.4.5 脆弱性识别

脆弱性识别也成为弱点评估，脆弱性是资产本身存在的，它可以被相应的威胁利用，引起资产或商业目标的损害。弱点包括物理环境、组织过程、人员、管理、配置、软硬件和信息

等各种资产的脆弱性。

单纯的脆弱性本身不会对资产造成损害，它只是一种条件或环境，可能导致被威胁利用造成资产损失。如果系统足够强健，严重的威胁也不会导致安全事件发生，并造成损失。所以威胁总是要利用资产的脆弱性才可能造成危害。资产的脆弱性具有隐蔽性，有些脆弱性只有在一定条件和环境下才能显现，这是脆弱性识别中最为困难的部分。不正确的、起不到应有作用的或没有正确实施的安全措施本身就可能是一个脆弱性。

脆弱性识别是风险评估中最重要的一个环节。脆弱性识别可以以资产为核心，针对每一项需要保护的资产，识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估，也可以从物理、网络、系统和应用等层次进行识别，然后与资产、威胁对应起来。脆弱性识别的依据是国际或国家安全标准和行业规范、应用流程的安全要求。

脆弱性评估是指通过技术检测、实验和审计等方法，寻找信息资产中可能存在的弱点，并对弱点的严重性进行赋值。在进行脆弱性评估时，提供的数据应来自于这些资产的拥有者或使用者，以及相关业务领域的专家和软硬件信息系统方面的专业人员。脆弱性评估采用的方法主要为工具扫描、手动审查、渗透测试、文档审查、人员询问和问卷调查等。

1. 脆弱性分类

脆弱性主要从技术和管理两个方面进行识别，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题，管理脆弱性可分为技术管理脆弱性和组织管理脆弱性两方面。对不同的识别对象，其脆弱性识别的具体要求应参照相应的技术或管理标准实施。对技术脆弱性，主要是通过本地和远程两种方式进行系统扫描、对网络设备和主机进行人工抽查，保证技术脆弱性的有效性和全面性。管理脆弱性识别可按照 GB/T 22081-2008《信息技术 安全技术 信息安全管理实用规则》对现有的安全管理制度及其执行情况进行检查，发现其中的漏洞和不足。

表 8.9 给出了一种脆弱性分类表。

表 8.9　脆弱性分类表

脆弱性分类	识别对象	包 含 内 容
技术脆弱性	物理环境	物理设备的场地、防火、供电、电磁防护、线路保护、机房防护和管理等方面
	网络结构	基础网络架构、网络传输加密、访问控制策略、网络设备安全漏洞和安全配置等方面
	系统软件	系统及应用软件的安全漏洞、物理保护、系统软件配置安全、软件安全功能、数据防护、系统管理等方面
	应用系统	应用系统的协议安全、数据完整性、访问控制、审计、鉴别机制、通信、密码保护等方面
管理脆弱性	技术管理	物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面
	组织管理	安全策略、组织安全、资产分类与控制、人员安全、符合性等方面

2. 脆弱性赋值

脆弱性的严重性主要是指可能引发的影响的严重性，因此与影响密切相关。关于技术脆弱性的严重性，一般都是指可能引发的影响的严重性，通常将之分为低、中、高 3 个等级。

1）低等级

一般指配置不规范、信息泄露等，可能会导致一些非机密性信息泄露、非严重滥用和误用等不太严重的影响。

2）中等级

介于低等级和高等级之间的脆弱性，一般不能直接被威胁利用，需要和其他弱点组合后才能产生影响。如果可以直接被威胁利用，只能产生中等影响。

3）高等级

可能导致超级用户权限被获取、机密系统文件被读写和系统崩溃等严重损害的影响。

脆弱性评估针对每一项需要保护的资产，找出每一种威胁可能利用的脆弱性，对脆弱性的严重程度进行评估，采用等级方式对已识别的脆弱性的严重程度进行赋值。

对某个资产，其技术脆弱性的严重程度还受到组织管理脆弱性的影响。因此，资产的脆弱性赋值还应参考技术管理和组织管理脆弱性的严重程度。

在实际工作过程中，可采用以下等级划分标准，即把资产的脆弱性严重程度分为5个等级，分别为可忽略、低、中等、高、很高，并且从低到高分别赋值为1～5，如表8.10所示。

在实际评估过程中，技术性弱点的严重性值一般参考扫描器中的值，并做适当修正，以获得适用的弱点严重性值。

脆弱性评估可以分别在管理和技术两个层面上进行，主要包括技术弱点检测网络架构与业务流程分析、策略与安全控制实施审计、安全弱点综合分析等。

表8.10 脆弱性严重程度赋值表

赋值	标识	说　明
1	可忽略	该弱点若被威胁利用，对资产造成的损失可以忽略，对业务基本无损害、只造成轻微或可忽略的影响
2	低	该弱点若被威胁利用，对资产造成较小的损失并立即可以控制影响
3	中等	该弱点若被威胁利用，对资产造成中等损失、业务受到中等程度的影响
4	高	该弱点若被威胁利用，对资产造成重大损失、业务中断等严重的影响
5	很高	该弱点若被威胁利用，可造成资产全部损失或不可用、持续业务中断等非常严重的影响

8.4.6 已有安全措施识别与确认

控制措施是在技术、管理和法律方面的管理风险的方法。包括策略、程序、指南、实践或组织结构。控制措施的目的是减少意外事件的发生或降低意外事件发生后的影响。

在识别脆弱性的同时，评估人员应对已采取的安全控制措施进行识别，并对其有效性进行确认，将有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。对确认为不适当的安全措施应检查是否应被取消，或对其进行修正，或用更合适的安全措施替代。

安全措施可以分为预防性安全措施和保护性安全措施两种。预防性安全措施可以降低威胁发生的可能性，如入侵检测系统。保护性安全措施可以减少因安全事件发生对系统造成的影响，如业务持续性计划、商业保险等。

对已有安全措施进行确认，不能简单了解使用了哪些安全产品或方法，应该从信息系统的各个层次对已有的安全机制进行确认，确认其安全强度是否达到了系统安全要求。一般

来说，安全措施的使用将减少系统技术或管理上的脆弱性，但安全措施确认并不需要具体到每个资产或组件的脆弱性，而是一类具体措施的集合，为风险处理计划的制定提供依据和参考。

8.4.7　风险分析阶段

在完成资产识别、威胁识别、脆弱性识别，以及对已有安全措施的识别和确认后，应进入风险分析阶段。风险分析的阶段的主要任务是风险分析和计算。

风险分析是根据资产识别、威胁识别、脆弱性识别的结果，计算实际的风险值。风险分析工作中，要对已有安全措施进行评价，在此基础上提出对风险处置的具体建议。风险处置的具体行为并不是风险评估的组成部分，它们共同组成了风险管理活动。

在完成了资产识别、威胁识别、脆弱性识别，以及已有安全措施确认后，将采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性。综合安全事件所作用的资产价值及脆弱性的严重程度，判断安全事件造成的损失对组织的影响。

1. 风险计算

风险可用下面的函数表示：

$$R = F(A, T, V, C)$$

其中，R 表示风险，A 表示资产，T 表示威胁，V 表示脆弱性，C 表示控制措施。但就计算方法而言，并没有成熟的方法。下面介绍一种风险计算方法。

风险的计算方法以下面的范式形式化加以说明。

$$M = F(A,T,V) = F(P(T,V), S(\mathrm{Ia}, \mathrm{Va}))$$

其中，M 表示风险值，F 表示安全风险计算函数，A 表示资产，T 表示威胁，V 表示脆弱性，P 表示威胁利用资产的脆弱性导致安全事件的可能性，Ia 表示安全事件所作用的资产价值，Va 表示脆弱性严重程度，S 表示安全事件发生后造成的损失。具体可分为 3 步。

1）计算安全事件发生的可能性

根据威胁出现频率及脆弱性的状况，计算威胁利用脆弱性导致安全事件发生的可能性，即

$$\text{安全事件发生的可能性} = P(\text{威胁出现频率}, \text{脆弱性}) = P(T,V)$$

在具体评估中，应综合攻击者技术能力、脆弱性被利用的难易程度和资产吸引力等因素来判断安全事件发生的可能性。攻击者技术能力包括专业技术程度、攻击设备等，脆弱性被利用的难易程度包括可访问时间、设计和操作知识公开程度等。

2）计算安全事件发生后造成的损失

根据资产价值及脆弱性严重程度，计算安全事件一旦发生后造成的损失，即

$$\text{安全事件发生后造成的损失} = S(\text{资产价值}, \text{脆弱性严重程度}) = S(\mathrm{Ia}, \mathrm{Va})$$

不同安全事件的发生对组织的影响也不同。部分安全事件的发生造成的损失既影响资产本身，又影响业务的连续性。在计算某个安全事件的损失时，应将对组织的影响考虑在内。对部分安全事件造成的损失的判断还应参照安全事件发生可能性的结果，对发生可能性极小的安全事件可以不计算其损失。

3）计算风险值

根据计算出的安全事件的可能性以及安全事件造成的损失，计算风险值，即

$$\text{风险值 } M = F(P(T,V), S(\mathrm{Ia}, \mathrm{Va}))$$

评估者可根据自身情况选择相应的风险计算方法计算风险值,如矩阵法或相乘法。

2. 风险结果的判定

风险结果的判定就是风险等级的划分。确定风险数值的大小不是组织风险评估的最终目的,重要的是明确不同威胁对资产所产生的风险相对值,即要确定不同风险的优先次序和等级,对于风险级别高的资产应被优先保护。可将风险等级分为5级,等级越高,风险越高。评估者也可根据被评估系统的实际情况自定义风险等级。表8.11提供了一种风险等级表。

表8.11 风险等级表

风险等级	标识	风险描述
1	可忽略	风险很低,对系统造成的影响几乎不存在,通过简单措施就可以弥补
2	低	风险较低,对系统造成的影响较低,通过一定手段很快能解决
3	中等	风险中等,对系统造成的影响中等
4	高	风险较高,对系统造成的影响严重,在一定范围内给组织造成损害
5	很高	风险很高,对系统造成的影响非常严重,严重影响组织运行

风险标准必须随着评估方法的确定实现确定,并在组织的信息系统安全方针文件中体现出来。在确定风险的可能性和影响时,应建立一个评估框架,通过它来确定风险情况,还应考虑到已有控制措施对威胁可能产生的阻碍作用。对风险进行等级化需要对可能性和影响做出定义,将可能性和影响分别分为高、中、低3个等级,用直观的矩阵形式来描述风险评价所依赖的风险的标准,将风险定义为高、中、低等级风险,建立概率—影响矩阵,即风险矩阵,如图8.5所示。

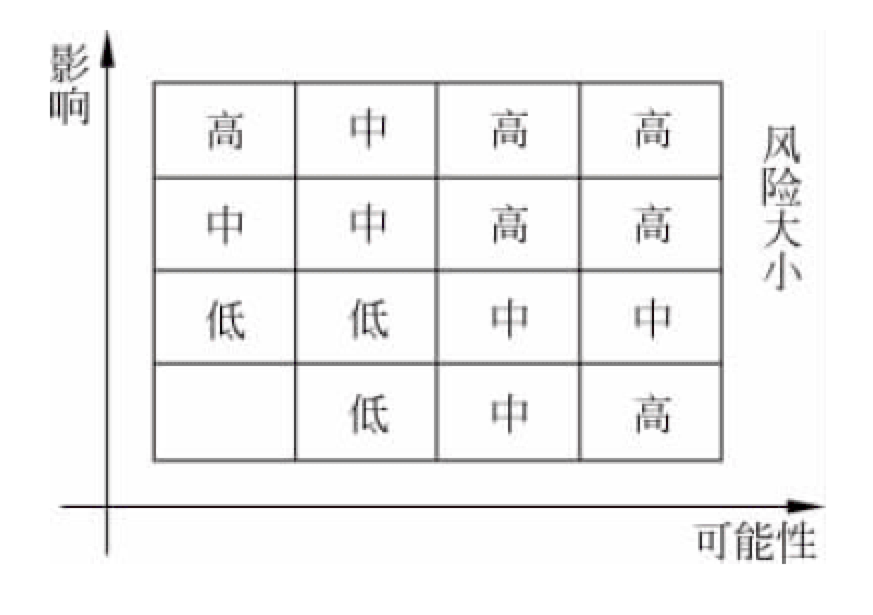


图8.5 风险矩阵

风险等级处理的目的是在风险管理过程中对不同风险进行直观比较,以确定组织安全策略。组织应当综合考虑风险控制成本与风险造成的影响,提出一个可接受的风险范围。某些资产的风险,如果风险计算值在可接受的范围内,则该风险是可接受的,应保持已有的安全措施;如果风险评估值在可接受的范围外,即风险计算值高于可接受范围的上限值,则该风险是不可接受的,需要采取安全措施以降低、控制风险。

3. 选择控制措施

对风险等级进行划分后,应考虑法律法规、机构自身的发展等要求以及风险评估的结果确定的水平,对不可接受的风险选择适当的处理方式制定风险处理计划。风险处理计划中应明确采取的弥补脆弱性的安全措施、预期效果、实施条件、进度安排、责任部门等。风险处理的方式包括回避风险、降低风险、转移风险、接受风险。风险处理的目的是直观地比较风险管理过程中的不同风险,确定组织的安全策略。组织应综合考虑风险控制成本与风险造成的影响,提出一个可接受的风险范围。

安全措施的选择应从管理与技术两个方面考虑。在风险处理方式及控制措施的选择上,组织应考虑发展战略、组织文化、人员素质等,并特别关注成本和风险的平衡,处理安全风险以满足法律法规及相关方的要求。安全措施的选择与实施应参照信息系统安全的相关标准进行。

4. 残余风险的评估

在对于不可接受的风险选择适当安全措施后,要对残余风险进行评估,以判断残余风险是否已经降低到可接受的水平。残余风险的评估可以依据组织风险评估的准则实施,考虑选择的控制措施和已有的控制措施对于威胁发生的可能性的降低。一般来说,安全措施的实施的目的是减少脆弱性或降低安全事件发生可能性,因此,残余风险的评估可以从脆弱性评估开始,在对照安全措施实施前后的脆弱性状况后,再次计算风险值的大小。

某些风险可能在选择了适当的安全措施后,残余风险的结果仍处于不可接受的风险范围内,应考虑是否接受此风险或进一步增加相应的安全措施。

8.4.8 风险评估结果的文档化

风险评估的过程需要形成相关的文件和记录,评估过程得到的所有结果都应写进风险评估报告中。风险评估报告的阅读者是信息资产的拥有者。该报告将帮助高层管理者和商业运营者在策略、商业过程、预算和改进管理等方面做出合理决策。

1. 文档化要求

记录风险评估过程的相关文件应符合以下基本要求,但不限于这些要求。

(1) 确保文件发布前已得到批准,确保文件是充分的。

(2) 必要时对文件进行评审,更新并再次批准。

(3) 确保文件的更改和现行状态可识别。

(4) 确保在使用时,可获得有关版本的适用文件。

(5) 确保文件的分发得到适当的控制。

(6) 确保文件保持清晰,易于识别。

(7) 防止作废文件的非预期使用,若因某种目的需保留作废文件时,应对这些文件进行适当标识。

对风险评估过程中形成的相关文件,还应规定其标识、存储、保护、检索、保存期限以及处置所需控制等。需要哪些相关文件及其详略程度由管理过程决定。

2. 风险评估文档类别

风险评估文件包括在整个风险评估过程中产生的评估过程文档和评估结果文档,包括但不限于以下基本文档。

1) 风险评估准备阶段

(1) 风险评估计划。

该计划阐述风险评估的目标、范围、组织机构、评估方法、经费预算、进度安排和评估结果的形式等。

(2) 风险评估程序。

程序中应明确评估的目的、职责、工作流程、输入数据、输出结果、相关文档及其要求,以及实施本次评估所需要的各种资产、威胁、脆弱性识别和判断依据。

2) 风险因素识别阶段

(1) 信息资产识别清单。

根据组织在风险评估程序文件中确定的资产分类方法进行资产识别,形成信息资产识

别清单，清单中应明确各资产的责任者或部门。

（2）重要信息资产清单。

根据资产识别和赋值结果，形成重要资产清单，记录重要资产的名称、描述、类型、重要程度、责任者或部门等。

（3）威胁列表。

根据组织的评估对象、环境等因素，形成威胁列表，包括威胁的名称、类型、来源、动机、出现频率等，为风险评估提供支持。

（4）脆弱性列表。

根据脆弱性识别和赋值结果，形成脆弱性列表，包括脆弱性的名称、类型、严重程度、描述等。

3）风险分析阶段

（1）已有安全措施确认表。

根据已有安全措施的确认结果，形成已有安全措施确认表，包括已有安全措施的名称、类型、功能描述、实施效果等。

（2）影响程度分析报告。

从资产损失和人员伤亡等方面，分析影响程度的大小。

4）风险等级评价阶段

（1）风险评估报告。

对整个风险评估过程和结果进行总结，说明组织的风险状况和残余风险状况，详细说明评估对象、评估方法、资产、威胁和脆弱性的识别结果、风险分析、风险统计、评估结论和建议等内容。通过管理层的评审，确定评估后的风险状况满足组织业务发展及相关方的要求。

（2）风险处理计划。

组织应针对评估结果中不可接受的风险制定风险处理计划，选择适当的控制目标和安全措施，明确责任、进度、资源，并通过对残余风险的评价确保所选安全措施的有效性。

（3）风险评估记录。

根据组织的风险评估程序文件，记录对重要信息资产实施的风险评估过程。要求风险评估过程中的各种现场记录可复现评估过程。记录应包括威胁、脆弱性的赋值及风险发生可能性的计算，已有安全措施的确认，风险值的计算与等级划分等。

上述文档均应通过组织管理层的批准，必要时应得到最高管理者的批准。

8.5 风险评估工具

风险评估工具是风险评估的辅助手段，是保证风险评估结果可信度的一个重要因素。风险评估离不开工具的支持，好的评估工具会给风险评估带来极大的科学性和方便性。风险评估工具的使用不但在一定程度上解决了手动评估的局限性，最主要的是它能够将专家知识进行集中，使专家的经验知识被广泛应用。

根据在风险评估过程中的主要任务和作用原理的不同，风险评估的工具可以分成风险评估与管理工具、系统平台风险评估工具、风险评估辅助工具 3 类。系统基础平台风险评估

工具主要用于对信息系统的主要部件(如操作系统、数据库系统、网络设备等)的脆弱性进行分析,或实施基于脆弱性的攻击。风险评估辅助工具则实现对数据的采集、现状分析和趋势分析等单项功能,为风险评估各要素的赋值、定级提供依据。

8.5.1　风险评估管理工具

1. 工具概述

风险评估管理工具是一套集成了风险评估各类知识和判断依据的管理信息系统,以规范风险评估的过程和操作方法。风险评估管理工具也可以用于收集评估所需要的数据和资料,基于专家经验,对输入输出进行模型分析。

风险评估管理工具大部分是基于某种标准方法或某组织自行开发的评估方法,可以有效地通过输入数据来分析风险,给出对风险的评价并推荐控制风险的安全措施。

风险评估管理工具实现了对风险评估全过程的实施和管理,包括被评估信息系统基本信息获取、资产、威胁和脆弱性的识别、风险计算、评估过程与评估结果管理等功能。评估可以通过问卷的方式,也可以通过结构化的推理过程,建立模型,输入相关信息,得出评估结论。通常这类工具在对风险进行评估后都会有针对性地提出风险控制措施。

根据实现方法的不同,风险评估管理工具可以分为 3 类。

1) 基于国际或国内标准的风险评估管理工具

国际和国内存在多种不同的风险分析标准或指南,不同的风险分析方法侧重点不同,以这些标准或指南的内容为基础,分别开发相应的评估工具,完成遵循标准或指南的风险评估过程。

2) 基于知识的风险评估管理工具

基于知识的风险评估管理工具遵循某个单一的标准或指南,并综合各种风险分析方法,结合实践经验,形成风险评估知识库,完成综合评估。

3) 基于模型的风险评估管理工具

基于模型的风险评估管理工具在对系统的组成部分、安全要素充分分析的基础上,对系统资产、威胁和脆弱性建立量化或半量化的模型。根据采集信息的输入,得到评估的结果。

2. 工具示例

根据以上对风险评估管理工具的分析,列出几种流行的风险评估管理工具。

1) COBRA

COBRA 是由 C&A 系统安全在 1991 年推出的用于风险评估的工具。COBRA 由一系列风险分析、咨询和安全评价工具组成,提供了一个完整的风险分析服务,并且兼容许多风险评估方法,如定性风险评估和定量风险评估等。COBRA 可看作是基于专家系统和知识库的问卷系统,它对所有的威胁和脆弱性进行评估,并给出合适的解决方案。它还对每个风险类别提供风险等级和风险分析报告。

2) CRAMM

CRAMM 是由英国中央计算机与电信机构(CCTA)的 ITIL 批准,由 Insight Consulting 在 1985 年开发的,后来又开发出几个主要版本。CRAMM 是结构化的包含在软件包中的过程,用于评估信息系统风险,并找出合适的解决方法。CRAMM 的评估结果是对当前风险

和建议的分析。

3）CORAS

CORAS 于 2003 年推出，它集成了大量的风险分析方法和模型、可复用经验包、支持方法应用的自动工具，并提供风险评估知识库和经验包知识库。CORAS 在描述评估目的时利用 UML 语言，交换风险评估数据时利用 XML 语言。

4）@RISK

@RISK 是 Palisade Corporation 推出的风险分析工具，它不是主要针对信息系统安全风险评估而设计的工具。它主要用于商业风险分析，为决策者提供策略等方面的分析。

此外，还有多种风险评估管理工具，此处不再赘述。

8.5.2 信息基础设施风险评估工具

信息基础设施风险评估工具主要用于对一些信息系统的部件，如操作系统、数据库系统、网络设备等的漏洞进行分析，它包括脆弱性评估工具和渗透性测试工具。脆弱性评估工具也称为安全扫描器或漏洞扫描器等，主要识别网络和主机系统脆弱性。这些工具能够发现软件和硬件中已知的安全漏洞，以决定系统是否易受已知攻击的影响。这些工具能够扫描网络、服务器、路由器、防火墙和应用程序，并发现其中的漏洞。

渗透性测试工具是根据漏洞扫描工具提供的漏洞进行模拟攻击测试，判断这些漏洞是否能被非法访问者利用的。这类工具通常包括黑客工具和脚本文件用于检测已发现的漏洞是否会给系统带来影响。通常渗透性工具与漏洞扫描工具一起使用，用于评估系统的深层次问题。

比较常用的信息基础设施风险评估工具包括 ISS Internet Scanner、Nessus、SAINT 等。在进行评估时，可以针对被评估对象的运行环境选择不同的工具。

8.5.3 风险评估辅助工具

这种工具在风险评估过程中必不可少，它用来收集评估所需要的资料和数据，这些数据的积累是风险评估科学性的基础。利用辅助工具可以帮助完成现状分析和趋势分析。

最常见的风险评估辅助工具是入侵监测系统，它通过对计算机网络或系统中的关键点收集信息并分析，以获取可能对网络或系统造成危害的入侵攻击事件，帮助检测各种攻击试探和误操作，同时也可以作为一个警报器，提醒管理员发生的安全状况。

同时安全审计工具、安全漏洞库、知识库都是风险评估不可或缺的支持手段。

8.6 风险评估方法

当前存在着许多风险评估的理论，这些方法遵循了基本的风险评估流程，在具体实施手段和风险计算方法上各不相同。评估方法的选择直接影响到评估过程中的每个环节，需要根据系统的具体情况，选择合适的风险评估方法。现在的风险评估方法有很多，可大致分为 3 类：定性风险评估、定量风险评估和综合风险评估。

8.6.1　定性风险评估方法

定性分析方法是采用较广泛的一种风险评估方法。它主要依据研究组的知识、经验、政策以及特殊变例等非量化的资料对系统风险状况做出判断的过程。该方法通常只关注威胁事件所带来的损失，而忽略事件发生的概率。多数定性风险分析依据组织面临的威胁、脆弱性以及安全措施等因素来决定风险等级。定性分析的操作方法多种多样，包括小组讨论、检查列表、问卷调查、人员访谈等，在此基础上，通过一个理论推断演绎的分析框架做出调查结论。

与定量评估方法相比，定性评估操作起来相对容易，它没有定量评估的计算负担，可以挖掘出一些蕴藏很深的思想，使评估的结论更全面和深刻。定性评估所需的时间、费用和人力资源较少，准确性也稍好。缺点是主观性很强，往往需要凭借分析者的经验和直觉，或者业界的标准和惯例，为风险管理诸要素的大小或高低程度定性分级，而且分析的结果也很难统一。另外，定性评估的精确性也不够。

下面介绍几种定性风险评估方法。

1. 初步风险分析

初步风险分析（Preliminary Risk Analysis，PRA）是一种定性分析方法，它用于定性分析事件序列，识别出哪些事件缺乏安全措施，这些潜在危害可能导致事故的发生。

通过初步风险分析方法，潜在的危险事件将逐一被识别出来，然后对其分别进行分析与评估。对每个危险事件或危害，其可能的改进或预防措施将被明确地表达出来。

根据初步风险分析方法产生的分析结果，确定需要进一步调查的危害以及分析方法，为决策提供基础。根据风险识别和风险分析结果对风险进行分级，并对可能的风险控制措施进行优先排序。

2. 危害和可操作研究

危害和可操作性研究（Hazard and Operability study，HAZOP）技术于 20 世纪 70 年代由英国皇家化学工业有限公司提出。HAZOP 分析是由专家组通过“头脑风暴会议”来进行，它是一种系统潜在危害的结构化检查方法。HAZOP 通过对新的或已有的设施进行系统化鉴定和检查，确定系统所有可能偏离正常设计的异常运行问题，并分析这种偏离正常运行的原因、可能性和可能造成的后果及后果的严重性，这种偏差是通过将一系列标准的引导词应用到正常的系统设计之上产生的，并最终影响到整个设施。引导词包括是/否（Yes/No）、大于/小于（More Than/Less Than），以及（As Well As）、相反的部分（Part of Reverse）等。分析出造成偏差的原因，采取适当的措施防止偏差的产生就可以防止系统失效以及可能引起的后果。HAZOP 分析方法的主要目标是发现存在的问题而不是解决问题。

3. 德尔斐法

德尔斐法是一种定性的预测方法，通过群体决策咨询的方法，群体成员各自独立工作，以系统独立的方式综合判断，克服某些权威左右的缺点，减少调查对象的心理压力，使预测的可靠性增加。德尔斐法的群体成员以非面对面的方式交流。德尔斐法进行风险分析的步骤如下：

（1）明确风险之后，群体成员填写精心设计的问卷，提出可能解决问题的方案，每个群

体成员匿名并独立完成第一份问卷。

(2) 把第一次问卷调查的结果在另一个中心地点整理出来,把整理出来的结果分发给每个人。

(3) 群体成员看分析整理结果,再次提出解决问题的方案,使原有的方案得到改善,或发现新的解决方法。

(4) 如果有必要,重复步骤(2)和步骤(3),直到发现合适的解决方法。

德尔斐法在评估分析过程中,保证群体成员不受他人影响,但是这种方法需要占用大量时间,在需要快速做出决策的情况下,此方法不再适用。

4. 故障模式影响及危害性分析

故障模式影响及危害性分析(Fault Mode Effect and Criticality Analysis,FMECA),于20世纪50年代由美国可靠性工程研究所提出,用于确定因军事系统故障而产生的问题。

FMECA由两部分工作组成:故障模式影响分析(Fault Mode and Effect Analysis,FMEA)和危害性分析(Criticality Analysis,CA)。FMECA是一种可靠性、安全性、维修性、保障性分析与设计技术,它是一种自底而顶的评估方法,按规定的规则记录系统设计中所有可能的故障模式,通过对系统中每个潜在的故障模式进行分析,以确定它对系统的影响,并按影响的严重程度进行分类。FMECA提出可能采取的改进措施,消除或减少故障发生的可能性,提供系统的可靠性和安全性。

8.6.2 定量风险评估方法

定量评估方法是一种比较精确的风险评估方法,通常以数学形式进行表达。当资料比较充分或者风险对信息资产的危害性可能很大、确有必要时可采用定量风险评估方法。定量评估方法对构成风险的各个要素和潜在损失的水平赋以数值,当度量风险的所有要素都被赋值,风险评估的整个过程和结果就可以进行量化。

进行定量风险评估的成本一般比较高。定量评估方法的优点是用直观的数据来表述评估的结果,而且比较客观,精确性好。定量分析方法的采用,可以使研究结果更科学、更严密、更深刻。缺点是常常为了量化,使本来比较复杂的事物简单化、模糊化,有的风险因素被量化以后还可能被误解和曲解,分析的准确性可能较差,需要大量的统计数据,操作复杂,计算量较大。

下面介绍几种常用的定量评估方法。

1. 模糊综合评价风险评估法

模糊综合评价是利用模糊数学中模糊线性变换原理和最大隶属度原则,考虑与被评价事物相关的各个因素,对其做出合理的综合评价。它是一种用定量的方法解决不确定、不完全信息的评价方法,其最大特点是可以比较自然地处理人类思维的主动性和模糊性。此方法特别适合解决那些只能用模糊的、非定量的、难以明确定义的实际问题。该种评估方法的着眼点是所考虑的各个相关因素。

2. 基于人工神经网络风险评估法

人工神经网络(ANN)是模拟人脑结构和思维过程,是一个高度自适应的非线性动态系统,具有记忆能力、自学习能力和联想能力,优点是人工干预少,精度较高,对专家知识的依

赖较少。主要用于解决不确定性、非结构性问题。神经网络中应用的最为广泛的是 BP 神经网络及其相应的组合网络，其特性是结构简单，可操作性强。

下面列出几种基于人工神经网络法评估方法。

1）基于 BP 神经网络的评估方法

反向传播神经网络(BP)是一种按误差反向传播算法训练的多层前馈网络，是目前应用最成熟的神经网络模型之一。数学理论已证明 BP 神经网络具有任意精度的函数逼近能力，所以，它为信息系统安全风险评估提供了一种可行的构造和表示方式。BP 神经网络是通过对所要解决的问题的知识存储以及对样本的学习训练，不断改变网络的连接权值以及连接结构，从而使网络的输出接近期望的输出的方法。这种方法的本质是对神经网络中的可变权值的动态调整。

基于神经网络的信息系统安全风险评估采用单隐含层的 BP 神经网络，其拓扑结构为输入层、隐含层和输出层。它的输入表示为特征量，即风险因素的各个评价指标，将这些指标经过量化处理和一致性处理后，作为 BP 神经网络的输入量。经过 BP 神经网络的学习算法，网络的输出特征量作为风险因素的风险级别。BP 神经网络的激励函数可以采用 Sigmoid 函数，隐含层单元数在训练过程中通过误判率的大小确定。

2）模糊神经网络评估方法

模糊神经网络是模糊理论与神经网络相结合的产物。神经网络的神经元不仅具有普通神经元的功能，同时又能反映神经元的模糊性质，具有模糊信息处理能力。模糊概念与神经网络相结合，将神经元输入引入模糊隶属度的概念，神经元仍保留原有形态和特性，输出层代表风险值的大小。基于模糊神经网络的信息系统安全风险评估法减少了人为因素的干扰，评价更加客观。

3）小波神经网络评估方法

小波神经网络将小波与 BP 神经网络相融合。基于小波神经网络的信息系统风险评估采用单隐含层的小波神经网络模型，将神经网络的输入表示为特征量，即风险因素的各个评价指标经量化和一致性处理后的量化值，经过小波神经网络的学习算法，网络的输出特征量为风险因素的风险级别。

3. 灰色系统理论

灰色系统理论是我国华中工学院学者邓聚龙教授于 1982 年创立。灰数是指缺少相关信息而在区间上不确定的数，用符号？表示。相对而言，已知确定的数称为白数，完全不知的数称为黑数。灰色系统将一切随机变量看作在一定范围内的灰色量，将随机过程看作是在一定范围内变化的与时间有关的灰色过程。对灰色量的处理不是从统计规律的角度通过大样本量进行研究，而是用数据处理的方法将杂乱的原始数据整理成规律性较强的生成数列再做研究。

引入白化权函数 $f(\otimes)\in[0,1]$，其中(0 为黑，1 为白)，以通常意义的灰度反映灰数区间各点的不确定性程度，其函数值 $f(\otimes)$ 称为灰数$\otimes$的白化值$\overline{\otimes}$。通过白化权函数，可以对区间上灰数进行各种运算。应用灰色系统理论可以建立对信息系统风险评估的定量评判算法。

灰色系统理论评估信息系统安全风险的基本步骤可以概括如下：

(1) 用累加和累减生成法处理原始生成数据。

(2) 依据生成数据建立灰色模型。

(3) 对确定的模型用残差检验法、后验差检验法或关联度检验法检验精度。

(4) 当精度符合要求时,可用灰色模型对信息系统安全风险进行分析与评估。

8.6.3 综合风险评估方法

在实际的系统风险评估过程中,系统风险评估是一个复杂的过程,需要考虑的因素很多,有些评估要素可以用量化的形式来表达,而对有些要素的量化又是很困难甚至是不可能的。因此不能将定性分析和定量分析两种方法简单地分开来,而要将这两种方法综合起来。在不容易获得准确数据的情况下采用定性分析方法分析,在定性分析的基础上使用定量方法进行计算以减少其主观性。定量分析是定性分析的基础和前提,定性分析建立在定量分析的基础上才能揭示客观事物的内在规律。

1. 层次分析法

层次分析法(Analytic Hierarchy Process,AHP)是由美国运筹学专家萨蒂教授于20世纪70年代提出的,首先在美国国防部的科研项目中取得应用,它是在网络系统理论和多目标综合评价方法基础上提出的一种层次权重决策分析方法。层次分析法在对复杂决策问题本质、影响因素及其内在关系等进行深入分析的基础上,利用较少的定量信息使决策思维过程数学化,从而为多目标、多准则、无结构特性、变量不易定量化的复杂决策问题提供了一种简便的决策方法,尤其是为决策结果难以直接、准确度量的场合提供了一种可有效将问题条理化、层次化的思维模式。

层次分析法的整个过程体现了人的决策思维的基本特征,即分解、判断与综合,且定性与定量相结合,便于决策者之间彼此沟通,是一种比较有效的系统分析方法,在信息系统安全风险分析与评估等众多领域得到了广泛应用。

2. 风险矩阵

风险矩阵由美国空军电子系统中心于20世纪90年代中期提出,并在美军武器装备系统研制项目的风险管理和控制中得到广泛应用。风险矩阵是用于识别风险影响程度的一种结构性方法,能够对潜在的风险进行评估,优点是操作简便,并结合了定性分析和定量分析。风险矩阵可以有多个栏目,如风险栏、威胁栏、影响栏、风险等级栏和风险管理栏等。每一栏目描述其要素对应的具体内容。

原始风险矩阵的各项组成确定后,就将相应的数据输入风险矩阵各项中。经过风险识别,识别出的潜在风险数量可能会很多,对系统的影响程度也不相同。经过风险分析,确定各风险的重要性,对风险进行排序并评估其可能产生的后果,有效控制风险。

风险识别和分析后,进行风险的定量分析。定量分析可以从风险影响程度和风险出现概率两个角度进行量化和分析。风险定量分析的目的是确定每个风险对系统的影响大小。

8.6.4 其他风险评估方法

风险评估方法的使用并不具有局限性,在不同领域中风险评估方法可以相互引用和借鉴,以下是在不同领域中其他几种常用评估方法。

1. 基于树的分析技术

1）故障树分析法

故障树分析(Fault Tree Analysis,FTA)的概念最初于 1962 年由贝尔实验室提出,最初是为分析 Minuteman 火箭系统而提出的一种可靠性的风险评估方法,随后广泛应用于航天工业、电子设备、化学工业、机械制造、核工业及一般电站。目前主要用于分析大型复杂系统的可靠性及安全性。

故障树分析(FTA) 是一种自顶而底的评估方法,采用树形图的形式,把系统的安全故障与组成系统的部件的故障有机地联系在一起。故障树分析通过对可能造成系统故障的硬件、软件、环境、人为因素进行分析,画出故障原因的各种可能组合方式或其发生概率,由总体至部分,按树状结构,逐层细化。故障树分析以系统不希望发生的事件作为目标,称为顶事件,按照演绎分析的原则,从顶事件开始逐级向下分析各自的直接原因事件,称为基本事件。在故障树分析方法中,关键在于故障树建模。故障树建模就是寻找系统故障与导致系统故障的因素之间的逻辑关系,并用故障树的图形符号抽象表示实际系统故障组合与传递的逻辑关系。图形符号包括事件符号与逻辑门符号。故障树建模完成之后，需要简化故障树,消除多余事件,以准确计算顶事件发生的概率。

2）事件树分析法

由于环境影响以及采取的安全措施不同,系统对初始事件有不同的响应方式,导致事件的发展过程与结果也不相同。因此应分析鉴别对不同响应导致的事件序列的发展过程。

事件树分析(Event Tree Analysis,ETA)起源于决策树分析(DTA),它是一种按事故发展的时间顺序由初始事件开始推论可能的后果,从而进行危险源辨识的方法。事件树分析在给定系统事件的情况下,分析此事件可能导致的各种事件的一系列结果,定性与定量地评价系统特性,帮助人们做出处理决策。

事件树分析是从一个初始事件开始,并描述了初始事件一切可能的发展方式与途径。它是一种时序逻辑的事故分析方法,它以一初始事件为起点,按照事故的发展顺序,分阶段,一步一步地进行分析,每一事件可能的后续事件只能取完全对立的两种状态之一的原则(如成功或失败、正常或故障、安全或危险等),逐步向结果方面发展,直到达到系统故障或事故点为止。所分析的情况用树枝状图表示,故叫事件树。事件树虽然列举了导致事件发生的各种事故序列组,但这只是中间步骤,不是最后结果。有了中间步骤才可以进一步整理初始事件与减少系统风险概率措施之间的复杂关系,并识别事故序列组所对应的事故场景。

3）因果分析法

因果分析(Cause Consequence Analysis,CCA)技术由丹麦 RISO 实验室开发,最初用于核电站的风险分析,后来它被推广应用于信息系统安全风险评估等众多领域,用于评估和保护系统的安全性。CCA 实际是一种故障树分析和事件树分析结合的方法,结合了原因分析(由故障树描述)和结果分析(由事件树分析)的特点。

CCA 的目的是识别出导致不希望发生结果的事件链。通过 CCA 图中不同事件的发生可能性,计算出各种后果的概率,从而确定系统的风险等级,并根据不同的风险等级采取不同的安全措施,保证系统的安全。

4）管理漏洞风险树

管理漏洞风险树(Management Oversight Risk Tree,MORT)由美国能源研究与发展

委员会于 20 世纪 70 年代提出，它能够与复杂的、面向目标的管理系统相协调。

管理漏洞风险树是一种将安全要素以有序的、符合逻辑的方式进行排列的图表。它利用故障树的方法来进行分析，最上层的事件是“破坏、损失、其他费用、企业信誉下降”等。管理漏洞风险树主要从管理漏洞角度给出了有关顶层事件发生原因的总体看法，从上层管理角度对风险进行分析和评估，并对风险管理与控制提出决策。

5）安全管理组织评审技术

安全管理组织评审技术（Safety Management Organization Review Technique，SMORT）是对 MORT 的简单修改。MORT 是基于完全的树结构，而安全管理组织评审技术通过对相关清单的分析来构建模型。从安全管理组织评审技术的结构分析过程来看，安全管理组织评审技术也是一种基于树的方法。

安全管理组织评审技术分析包括基于清单和相关问题的数据收集与结果赋值。上述信息可以通过调研、对文件的研究等来收集。通过安全管理组织评审技术能够完成对意外事件的详细调查，并可用于制定安全审计和安全度量计划。

2. 基于动态系统的技术

1）GO 方法

GO 方法（GO Method）由 Kaman 科学公司于 20 世纪 70 年代提出，首先在美国国防部的电力系统可靠性和安全性分析得到应用，是一种面向成功逻辑的系统分析方法。

GO 方法通过工程图来构建 GO 模型，在模型构建中它使用了 17 个算子，使用一个或多个 GO 算子代替系统中的元素。

GO 算子有 3 种基本类型：独立算子、依靠算子和逻辑算子。

独立算子用于无输入部门的建模；依靠算子至少需要一个输入，才能有一个输出；逻辑算子将算子结合在一起，形成目标系统的成功逻辑。

基于独立算子和依靠算子的概率数据，可以计算出成功操作的概率。在实际应用中，通过适当的方法定义目标系统的边界条件时，可使用 GO 方法对系统的风险和安全性进行分析和评估。

2）有向图/故障图

有向图/故障图（Digraph/Fault Graph）方法使用图论中有关的数学方法和语言对系统的风险和安全性进行分析，如路径集和可达性。

此方法使用“与门和或门”（AND/OR）。来自系统邻接矩阵的连通矩阵显示一个故障节点是否会导致顶事件的发生，对这些矩阵进行分析，得出系统的单态或双态。单态指造成系统故障的单个因素，双态指造成系统故障的两个因素。

此方法允许形成循环、反馈，这样在对动态系统进行风险分析与评估时具有较大的吸引力。

3）马尔可夫分析法

马尔可夫（Markov）分析法提供了事件驱动型系统可靠性、可用性和安全性的分析方法，适合于需要考虑系统状态的情形。其他一些系统分析方法通常假定系统的组件是相互独立的，此方法假设系统的各个组件之间可以有较强的相互依赖关系。

马尔可夫分析方法包括马尔可夫链和马尔可夫过程两种基本方法。马尔可夫链是一个随机变量序列，将来的随机变量只取决于当前的随机变量，与当前随机变量之前的其他随机

变量无关。这与其他随机事件是不同的，因为在很多随机事件中，将来的事件发生是受到以前发生事件的影响的，它们前后存在着较大的相关性，不是相互独立的。马尔可夫链分为齐次马尔可夫链和非齐次马尔可夫链。齐次马尔可夫链的状态间转移率是常量，与事件无关，而非齐次马尔可夫链的状态间转移率是变量，是时间的函数。马尔可夫过程的基本假设是每个状态系统的行为都不会被记忆。马尔可夫过程完全由其转移概率矩阵所确定。一个无记忆系统的将来状态只取决于其当前状态，与过去无关。一个稳定系统的状态转移概率不随时间变化。

马尔可夫模型根据系统的初始配置状态。估计从一个已知状态转移到下一逻辑状态的概率，直到系统达到一个最终或完全失效的状态。在马尔可夫分析方法中，利用状态转移图这种形象、直观的方式描述系统所有离散状态和状态间可能的转移途径，状态间的转移频率仅仅取决于当前状态的概率和状态间的固定转移率。马尔可夫状态转移过程可使用差分方程来表示，差分方程阶数等于状态的数目。

马尔可夫方法适宜分析比较小的系统，当分析大型系统时，马尔可夫状态转移图很大且复杂，比较难构造，但可以与 FTA 和 FMECA 综合使用分析复杂系统。

4）动态事件逻辑分析方法

动态事件逻辑分析方法（Dynamic Event Logic Analytical Methodology，DELAM）提供了一个用于对时间、过程变量和系统的精确处理的完整框架。

动态事件逻辑分析方法通常包括 4 个步骤：系统组成部分建模；系统方程求解算法；设置最高条件；时间序列产生和分析。

动态事件逻辑分析方法对系统的可靠性、安全性进行评估，并对系统的行为、活动进行识别，在描述动态事件方面非常有用。在对某个特定问题进行分析时，需要建立系统的 DELAM 模拟器，然后提供各种输入数据。输入数据可以是在特定条件下系统组成部门的发生概率、概率的独立性、不同状态间的转换率、状态与过程变量的条件概率矩阵等。

5）动态事件树分析方法

动态事件树分析方法（Dynamic Event Tree Analysis Method，DETAM）是基于时间变化要素的方法，时间变化要素包括设备硬件状态、过程变量值和事件发生过程中的操作状态等。一个动态事件树也是事件树，只是分支于不同的时间点上。

动态事件树分析方法通过 5 个特征集来定义，分别是分支集、变量集、分支规则、序列扩张规则和量化工具。

分支集用于确定事件树节点可能的分支空间；变量集定义系统状态；分支规则用于确定什么时候发生分支；序列扩张规则用于限制序列的数量。

动态事件树分析方法可用于表示操作行为的多样化、建立操作行为的结果模型、分析使用因果模型的框架以及分析与评估紧急的安全事件及其过程变化，以判断在哪里进行改变、怎样进行改变能达到比较好的控制效果。

上面对几种常见的风险评估方法进行了介绍。它们各有优缺点，适用于不同的条件和场合。在实际的信息系统安全风险评估工作中，根据需要，灵活、综合运用这些技术和方法，以取得最佳的评估结果。

8.7 典型的信息系统安全风险评估方法

上节介绍了风险评估的方法,本节继续介绍几种典型的信息系统安全风险评估方法。

8.7.1 OCTAVE 方法

可操作的关键威胁、资产和脆弱性评估(Operationally Critical Threat、Asset and Vulnerabilityn Evaluation,OCTAVE)是由美国卡耐基·梅隆大学软件工程研究所开发的基于风险策略和计划的信息系统安全风险评估方法,其包括 OCTAVE 框架、OCTAVE 方法、OCTAVE 标准,这些文件不仅是信息系统安全风险评估的基本框架规范,也说明了如何具体实施 OCTAVE 方法的样本、工作表和使用说明。基本框架规范定义了一系列原则、属性和输出、样本、工作表和使用说明指导实施风险评估。

OCTAVE 方法适合正在寻求和理解自身安全需要的组织。OCTAVE 方法是自引导式的,要求组织内部的人员负责制定组织的安全策略。此技术要求组织内部人员对信息系统安全的实践和过程进一步了解,获得组织当前的安全状况。对关键资产的评估结果可用来确定修改的先后顺序和调整组织的安全策略。

OCTAVE 方法关注的是组织的风险、策略和与实践相关的问题。它是一种很灵活的评估方式,可以适合大多数组织。使用 OCTAVE 方法时,来自业务部门和 IT 部门的评估人员组成评估小组,陈述组织的安全需求,在操作风险、安全实践和技术 3 个方面进行权衡。

OCTAVE 方法由操作风险和安全实践驱动。通过 OCTAVE 方法评估,组织要基于信息资产的机密性、完整性和可用性的风险做出信息保护方案。

1. OCTAVE 方法的主要特点

1) OCTAVE 方法是自引导的

要求组织管理评估过程并做出相应的信息保护决定。评估小组领导评估的整个过程。

2) OCTAVE 方法是由资产驱动的评估方式

OCTAVE 方法提出的风险评估是以资产驱动,并结合威胁和脆弱性评估的。评估小组识别组织的关键信息资产,并对其进行风险分析。

OCTAVE 的核心是自主原则,即由组织内部的人员管理和指导该组织的信息系统安全风险评估。信息系统安全是组织内每个人的职责,而不只是信息部门的职责。OCTAVE 首先强调的是 O(可操作性),其次是 C(关键性)。

OCTAVE 的关键结果包括组织改进其安全状态的保护策略和减少组织的关键资产的风险的缓和计划。评估结果仅为组织改进安全状态指明了方向,但不一定有重大改进。为了有效地管理信息系统安全风险,必须根据风险评估的结果开发详细的行动计划,并对这些计划的实施进行管理。OCTAVE 方法的评估结果包括 3 种类型的输出数据:组织数据、技术数据和风险分析与缓解数据。

OCTAVE 方法为大型组织而设计,对于规模较小的组织可以使用 OCTAVE-S 方法。

2. OCTAVE 方法的主要过程

OCTAVE 方法包括 3 个阶段共 8 个过程,每个阶段包含的过程描述如下。

1) 阶段一：建立基于资产的威胁描述

此阶段从组织角度进行评估。评估小组决定哪些组织的资产重要和已实施安全措施的信息资产。负责分析的团队对这些信息进行整理,以确定对组织的关键资产,并标识对关键资产的威胁,建立威胁描述文件。该阶段包括 4 个过程。

(1) 过程 1：标识高层管理部门的信息。

评估小组从有代表性的高级管理部门处收集有关重要资产、安全要求、威胁、目前组织的安全实践和组织脆弱性的信息。

(2) 过程 2：标识业务领域管理部门的信息。

评估小组从主管选定的业务领域管理部门处收集有关重要资产、安全要求、威胁、目前组织的安全实践和组织脆弱性的信息。

(3) 过程 3：标识员工的信息。

评估小组从业务领域管理部门的普通员工处收集有关重要资产、安全要求、威胁、目前组织的安全实践和组织脆弱性的信息。

(4) 过程 4：建立威胁描述。

评估小组选择几个关键资产,提炼关键资产的安全需求,为它们建立威胁描述文件。

2) 阶段二：确定基础设施的脆弱性

该阶段对基层设施进行评估,分析用于支持每种关键资产的系统组件,找出导致影响关键资产执行的脆弱性。该阶段包括两个过程。

(1) 过程 5：确定关键组件。

识别出用来支持和处理关键信息相关的资产系统中关键组件的类型,确定它们的评估方式。

(2) 过程 6：评估选定的组件。

运行脆弱性评估工具,评估选定的基础设施组件,并分析评估结果,精练关键资产的威胁描述。

3) 阶段三：制定安全策略和计划

分析团队评估组织中关键资产的风险,并确定需采取的措施。依据对收集信息的分析结果,为组织制定保护策略和风险削减计划。该阶段包括 2 个过程：

(1) 过程 7：实施风险评估。

标识关键资产的威胁影响,制定风险评估标准,决定威胁对组织的影响值。所有存在的风险都应进行评估。

(2) 过程 8：制定保护策略。

评估小组制定整个组织的保护策略,该策略注重于提高组织的安全实践,以及关键资产的风险削减计划。

OCTAVE 方法的主要过程如图 8.6 所示。

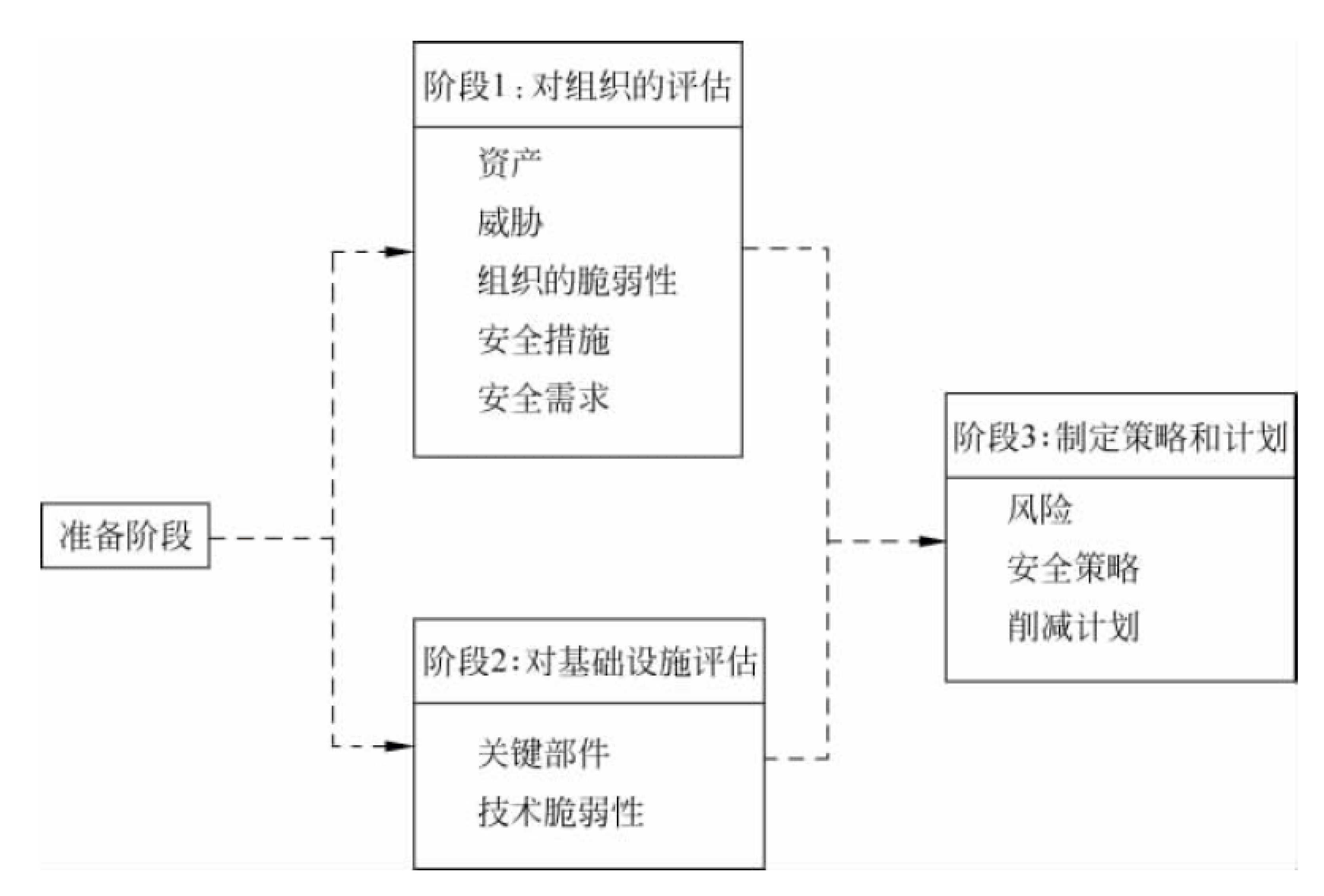


图 8.6 OCTAVE 方法的主要过程

8.7.2 层次分析法

1. 层次分析法的基本原理与主要步骤

层次分析法的基本思想是在决策目标的要求下，根据所要分析的问题的性质和达到的总体目标，将问题分解为不同的组成因素，并按照因素间的相互关联、影响以及隶属关系将因素按不同的层次聚集组合，形成一个层次的分析结构模型，并最终把系统分析归结为最底层相对于最高层的相对重要性权值的确定或相对优劣次序的排序问题。

层次分析法是一种定性分析与定量分析相结合的多目标决策分析法，这一方法的核心是将决策者的经验判断进行量化，为决策者提供定量形式的决策依据。由于层次分析法在许多目标决策问题方面具有优势，目前已在许多领域得到广泛应用。

层次分析法的分析流程如图 8.7 所示。

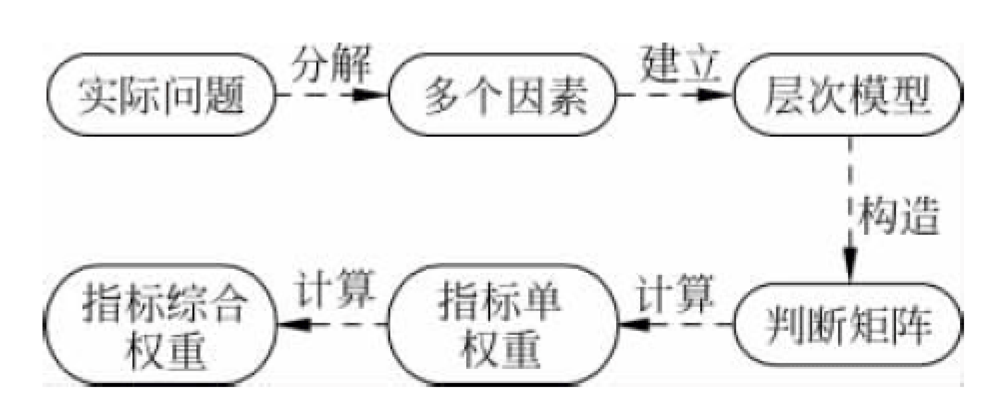


图 8.7 层次分析法的分析流程

层次分析法的基本步骤是：

1）系统分解，建立层次结构模型

层次模型的构建基于分解法的思想，进行对象的系统分解。建立层次结构模型的目的是在深入分析实际问题的基础上，建立基于系统基本特征的评估指标体系。具体地说，首先需要对系统进行分析，将复杂问题分解为由多个元素组成的子部分，再将这些元素按属性分成若干组，形成不同层次，同一层次的元素作为准则对下一层的某些元素起支配作用，同时又受上一层元素的支配。层次结构模型的基本层次有目标层、准则层和方案层，如图 8.8 所

示。目标层是指评估的最终目标。准则层是指影响目标实现的准则，它是联系上下层的中间环节，既要保证目标层的实现，又要保证方案层的优劣能得到正确合理的评判。方案层是指促使目标实现的方案，其中的每一个要素代表着一个参评方案。其中，准则层可以由若干个层次组成，包括所需考虑的准则、子准则。

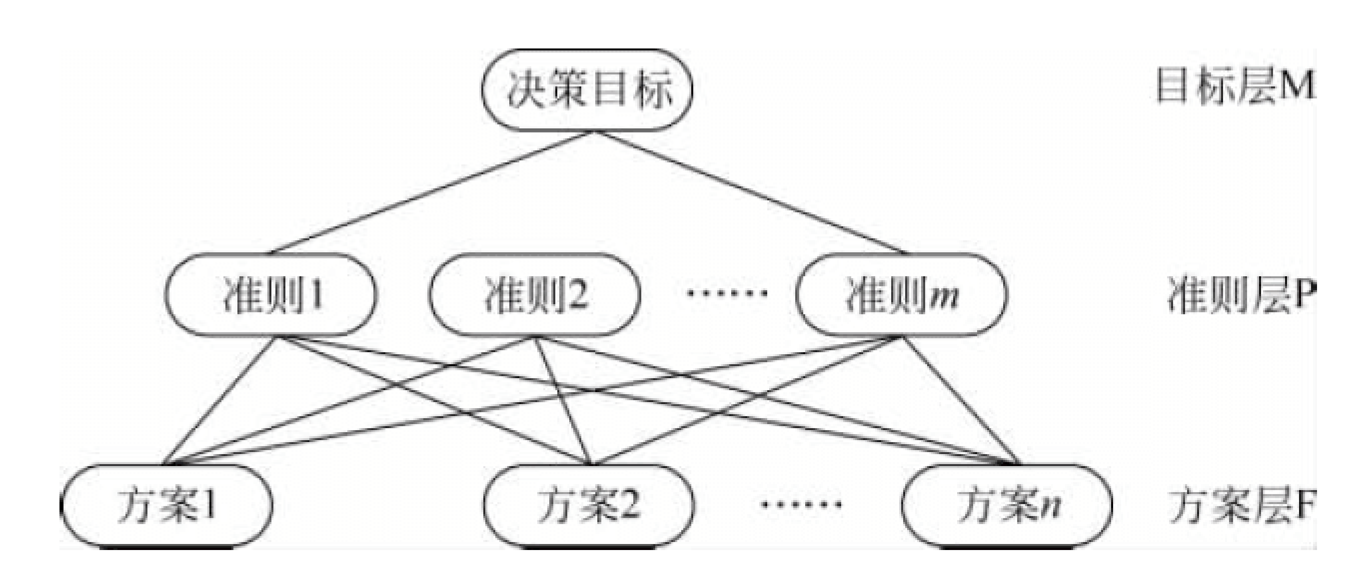


图 8.8　层次结构模型

2）构造各层次的判断矩阵

在建立层次结构模型之后，上下层之间的元素的隶属度就确定了，可以构造一系列判断矩阵。判断矩阵是将层次结构模型中同一层次的要素相对于上层的某个因素，根据重要程度相互间进行成对比较而形成的矩阵。判断矩阵的作用是在上一层某一元素的约束条件下，对同层次的元素之间的相对重要性进行比较。在对评估指标的相对重要程度进行测量时，引入 9 分位的相对重要的比例标度，构成一个判断矩阵，重要性标度值如表 8.12 所示。

表 8.12　1～9 标度

重要性标度	含　　义
1	表示元素 i 与元素 j 相比，两者同样重要
3	表示元素 i 与元素 j 相比，前者比后者稍重要
5	表示元素 i 与元素 j 相比，前者比后者明显重要
7	表示元素 i 与元素 j 相比，前者比后者强烈重要
9	表示元素 i 与元素 j 相比，前者比后者极端重要
2、4、6、8	表示上述相邻判断的中间值
$1/a$	表示若元素 i 与元素 j 的重要性之比为 a，则 j 与 i 的重要性之比为 $1/a$

设某层有 n 个元素，要比较它们对上一层某一准则(或目标)的影响程度，确定在该层中相对于某一准则所占的比重，即把 n 个元素对上层某一目标的影响程度排序。上述比较是同一层中两两元素之间进行的比较，比较时取 1～9 尺度。例如，方案 1，方案 2，……，方案 n 与上一层准则 P 有关联。建立这几个方案关于准则 C 的判断矩阵如下：

$$\boldsymbol{M}=(m_{ij})_{n\times n}=\begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ m_{21} & m_{22} & \cdots & m_{2n} \\ \vdots & \vdots & & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{nn} \end{bmatrix}$$

其中，$m_{ij}>0$，$m_{ii}=1$，$m_{ij}=\dfrac{m_{ik}}{m_{jk}}$，用 m_{ij} 表示第 i 个元素相对于第 j 个元素的比较结果，则 $m_{ij}=1/m_{ji}$。

m_{ij} 表示对于准则 P 而言，方案 i 与 j 比较而得到的相对重要程度或优越性。m_{ij} 的取值是根据资料、统计数据、征求专家意见以及系统分析员的经验而确定的。

3）判断矩阵计算及一致性检验

这一过程称为层次单排序，判断矩阵 $\boldsymbol{M}$ 对应与最大特征值 λ_{max} 的特征向量 w，经归一化后，为同一层次相应因素对应于上一层次某因素相对重要性的排序权值进行排序。对判断矩阵进行数学计算，求其主特征值及其相应的主特征向量，该向量即为层次单排序结果。构造判断矩阵的办法虽然较客观地反映出一对因子影响力的差别，但综合全部比较结果时，难免包含一定程度的非一致性，为了检验构造出来的判断矩阵是否具有严重的非一致性，以便确定是否接受该判断矩阵，还要对判断矩阵进行一致性检验。

判断矩阵的运算和一致性的检验具体过程如下：

（1）最大特征值具体计算方法。

① 将判断矩阵的每一列元素作归一化处理，其元素的一般项为

$$\overline{m_{ij}} = \frac{m_{ij}}{\sum_{k=1}^{n} m_{kj}} \quad (i,j = 1,2,\cdots,n) \tag{8-1}$$

② 对各列归一化后判断矩阵按行相加

$$\overline{w_i} = \sum_{j=1}^{n} \overline{m_{ij}} \quad (i,j = 1,2,\cdots,n) \tag{8-2}$$

③ 相加后的向量再归一化处理，所得的结果即为所求特征向量

$$w_i = \frac{\overline{w_i}}{\sum_{j=1}^{n} \overline{w_j}} \quad (i,j = 1,2,\cdots,n) \tag{8-3}$$

④ 通过判断矩阵 $\boldsymbol{M}$ 和特征向量 $\boldsymbol{w}$ 计算判断矩阵的最大特征值 λ_{max}。

$$\lambda_{max} = \sum_{i=1}^{n} \frac{(\boldsymbol{Mw})_i}{n w_i} \quad (i,j = 1,2,\cdots,n) \tag{8-4}$$

其中 $(\boldsymbol{Mw})_i$ 代表向量 $\boldsymbol{Mw}$ 的第 i 个元素。

（2）进行一致性检验。

① 一致性指标

$$\mathrm{CI} = (\lambda_{max} - n)/(n-1) \tag{8-5}$$

其中，n 为判断矩阵的阶数。

② 选择随机一致性指标 RI。

对于 1～9 阶矩阵，RI 见表 8.13。

表 8.13 随机一致性指标

阶数	1	2	3	4	5	6	7
RI	0	0	0.58	0.90	1.12	1.24	1.32
阶数	**8**	**9**	**10**	**11**	**12**	**13**	**14**
RI	1.41	1.45	1.49	1.52	1.54	1.56	1.58

③ 计算一致性指标

$$CR = CI/RI \tag{8-6}$$

若 CR<0.1,认为判断矩阵具有满意一致性,否则对判断矩阵进行调整。

4) 层次总排序及一致性检验

层次总排序是指每一个判断矩阵各因素针对目标层的相对权重,即将上一步计算得到的单排序结果进行适当组合,计算最下层对目标层的组合权向量。

最后做组合一致性检验,若检验通过,则可按照组合权重向量表示的结果进行决策,否则需要重新考虑模型或重新构造那些一致性比率大于 0.1 的成对比较阵。

8.7.3 FTA

故障树分析法可分为定性和定量两种方式。故障树的定性分析是通过求故障树的最小割集,得到顶事件的全部故障模式,发现系统结构中的最薄弱环节和关键点,集中对最小割集所发现的关键点进行强化。定性分析和定量分析都需要有以下两个基本步骤。

1. 建立故障树

顶事件是重大风险事件,顶事件是由于若干中间事件的逻辑组合导致的,中间事件是由于各个底事件逻辑组合导致的。表示结果的顶事件在上,表示原因的底事件在下,中间层是下层事件的结果和上层事件的原因,这样构成了一个倒立的树状逻辑因果关系图。

图 8.9 给出了一种故障树。事件 1 是顶事件,造成事件 1 发生的原因是事件 2 或者是事件 3。事件 2 是一个中间事件,它既是事件 1 的原因,也是事件 4 和事件 5 的结果。事件 2 是事件 4 和事件 5 共同作用的结果。

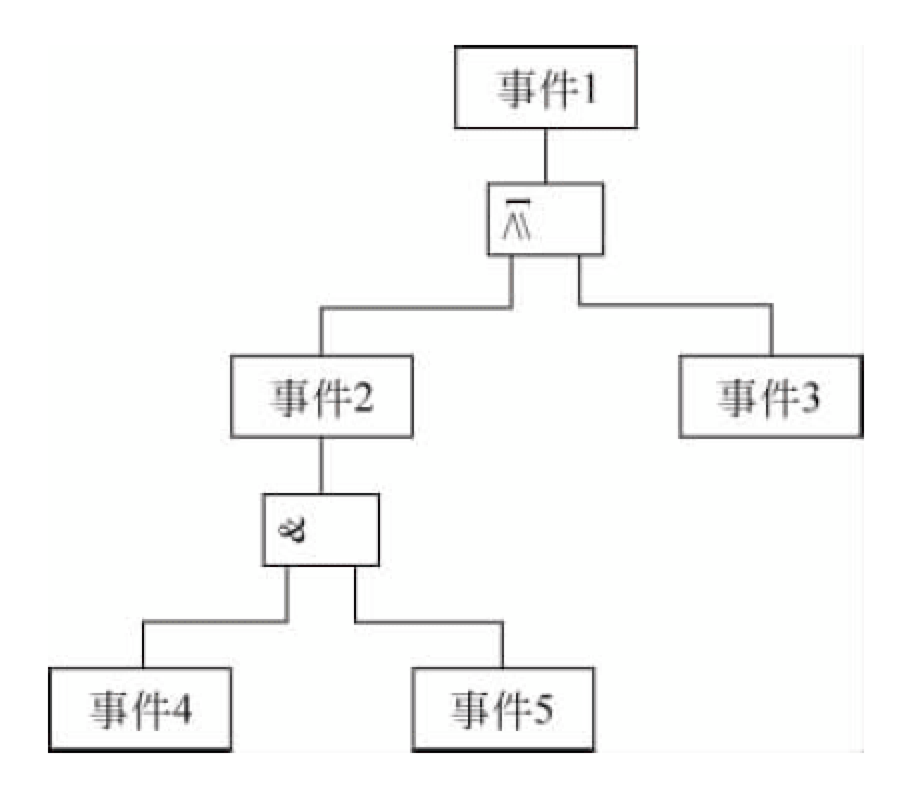


图 8.9　故障树示例

2. 简化故障树,求出故障树的全部最小割集

割集是指故障树中导致顶事件必然发生的一些底事件的集合。若在某个割集中将任意一个底事件去掉,余下的底事件不能构成割集,即不能使顶事件必然发生,则这样的割集就是最小割集。

8.7.4 威胁分级法

此方法通过分析威胁、威胁对资产的影响以及威胁发生的可能性来确定风险。威胁分级法首先要确定威胁对资产的影响,用等级进行表示。识别威胁的过程可以通过准备威胁列表,让用户去选择确定相应的资产威胁,也可以由分析团队人员来确定相关的资产威胁,而后进行分析与归类。然后评价威胁发生的可能性。在确定威胁的影响值和威胁发生的可能性后,计算风险值。

风险值的计算方法可以是影响值与可能性之和,也可以是之积,具体算法由用户确定,只要满足是增函数即可。

本例可以将威胁的影响值和威胁发生的可能性均分为5个等级，风险值的计算采用两值的积，具体计算如表8.14所示。在具体评估中，可以根据该方法来明确表示“资产—威胁—风险”之间的对应关系。

表8.14 威胁分级法

资产	威胁描述	影响值	威胁发生可能性	风险值	风险等级
某个资产	威胁1	4	4	16	2
	威胁2	3	4	12	3
	威胁3	5	5	25	1
	威胁4	1	2	2	5
	威胁5	2	4	8	4
	威胁6	3	3	9	4

8.7.5 风险矩阵测量

此方法的特点是事先建立资产值、威胁等级和脆弱性等级的对应表。对每个资产面临的风险都考虑其资产值、威胁等级和脆弱性等级，即预先定义好其风险等级。对应表如表8.15所示。

表8.15 资产值、威胁等级、脆弱性等级对应表

资　产　值				1	2	3	4	5
威胁等级	低	脆弱性等级	低	1	2	3	4	5
			中	2	3	4	5	6
			高	3	4	5	6	7
	中	脆弱性等级	低	2	3	4	5	6
			中	3	4	5	6	7
			高	4	5	6	7	8
	高	脆弱性等级	低	3	4	5	6	7
			中	4	5	6	7	8
			高	5	6	7	8	9

如果资产值为2，威胁等级为中，脆弱性等级为中，查表可知风险值为4。由表8.15可以推出，风险矩阵会随着资产值的增加、威胁等级的增加和脆弱性等级的增加而增加。

若某一资产由若干子资产组成，可以分别计算子资产所面临的风险值，接着计算总值。假设某系统有3种资产 $A1$，$A2$，$A3$，系统存在威胁 B。设资产 $A1$、$A2$、$A3$ 的值分别为2、3、4，对于 $A1$ 和 B，威胁等级为中，脆弱性等级为低，则 $A1$ 的风险值为3，同样对于 $A2$ 和 B，威胁等级为高，脆弱性等级为中，则 $A2$ 的风险值为6。对于 $A3$ 同样计算。那么此系统的总的风险值可以用下面的式子表示：

$$\text{系统的总风险值} = A1 \times B + A2 \times B + A3 \times B$$

这样可以实现对不同系统的比较，以便确定优先级，并在同一系统内做好资产的划分。

8.7.6 风险综合评价

风险的大小由威胁产生可能性、威胁对资产的影响程度以及已采用的控制措施3个方

面来确定。

风险综合评估方法中重要的是威胁类型的识别。通常首先需要建立一个威胁列表，然后进行资产识别，接着识别威胁以及威胁产生的可能性，最后对威胁造成的影响进行分析。

威胁的影响可以分为对人员的影响、对业务的影响和对财产的影响等。在考虑这些影响时，假定不存在控制措施，将上述各值相加后填入表中。可以将威胁的可能性和威胁的影响均分为 1～5 级。确定威胁的可能性和威胁的影响后，计算总的影响值。表 8.16 中采用了简单加法。在具体评估中，可以由用户根据具体情况来确定计算方法。

最后分析是否采用了能够减小威胁的控制措施，包括从外部保障的和从内部建立的控制措施，并确定其有效性、对其进行赋值。表 8.16 中，将控制措施的有效性分为 1～5 等级。在此基础上，根据公式求出总值，即为风险值。

表 8.16　风险评估表

威胁类型	可能性	对人的影响	对财产的影响	对业务的影响	影响值	已采用的控制措施		风险值
						外部	内部	
威胁 1	4	1	1	2	8	2	2	4
威胁 2	3	2	1	1	7	3	3	6
威胁 3	5	2	3	1	11	1	1	2

8.8　本章小结

本章介绍了信息系统安全风险评估的基础知识。首先介绍了风险评估的相关概念、意义和内涵，然后介绍了风险评估的相关标准和风险评估工具。接着简要介绍了风险评估的两种方式。详细分析了风险评估的基本步骤及其各步骤的主要任务。在介绍风险评估方法的基础上，详细地对典型的信息系统安全风险评估方法进行了分析。

8.9　习　题

1. 简要说明风险分析的过程。
2. 简略介绍几种风险评估的标准。
3. 风险评估的方式有哪些？并简要说明。
4. 试比较定性风险评估和定量风险评估的优缺点。
5. 风险评估的工具有哪些？并简要说明。
6. 简述层次分析法的主要步骤。

第 9 章　信息系统安全示例

9.1　电子政务信息系统安全示例

电子政务信息系统是政府综合运用计算机和网络技术，将党政机关的办公业务和公文流转转移到网络平台，以实现党政事务的公开、透明、高效，并促进以信息的共享为目的的综合信息系统的发展。电子政务系统通常包含两大部分：内部政务办公系统和对外服务部分。通常情况下，电子政务系统中内部办公系统的数据中涉及政府机密信息，由于网络的开放性与共享性，网络中的诸多不安全因素必然会影响到电子政务信息系统内部的安全。按照密级最大化原则，一般的电子政务网都是涉密网，所以要严格按照涉密信息系统的建设要求进行规划建设。因此，为了确保电子政务信息系统功能的正常发挥，防止信息系统中安全事件的发生，需要在分析电子政务信息系统风险及需求的基础上，进行安全规划与设计，从而建立一套完整的安全解决方案或安全保障体系。

9.1.1　系统风险分析

电子政务信息系统是党政机关的信息处理系统，存在一些国家及政治上的敏感信息，因此电子政务系统必然存在一定的安全风险。安全风险分析主要是对系统资源、威胁及脆弱性的分析，是电子政务信息系统安全规划与建设的前提。我国电子政务信息系统的安全性系数比较低，安全防御能力十分脆弱。总体来说，电子政务信息系统的安全风险来自于技术、管理、法律法规以及安全意识等方面。

风险分析将涉及几个重要的参数，包括威胁发生的可能性、危害程度、威胁与危害程度之间的关系等。进行安全风险分析时需要建立风险分析模型，以求能够定性并定量地描述风险、威胁及脆弱性。但是目前还没有一个普遍适用的风险分析量化模型，因此很难完成对电子政务信息系统风险的量化分析。尽管如此，通过分析系统所面临的各种安全威胁，仍然可以通过定性的方法准确定位到安全风险的分布、危害程度及解决方法。

1. 安全威胁分析

电子政务信息系统安全策略可以根据安全威胁发生的可能性等级进行制定与实施。电子政务信息系统安全威胁发生的可能性可以划分为 4 个等级：Ⅰ、Ⅱ、Ⅲ、Ⅳ级威胁。其中Ⅰ级表示肯定会发生的威胁，必须要予以考虑；Ⅱ级表示可能会发生的威胁，应予以考虑；Ⅲ级表示可能发生的威胁，但可以暂缓考虑；Ⅳ级表示基本不会发生的威胁，可以暂时不考虑。

2. 网络攻击分析

由于电子政务信息系统的信息和用户具有国家特性，因此可能受到来自于间谍、恐怖分

子、专业罪犯、黑客、内部人员、蓄意破坏者等人员的攻击，攻击发生的可能性大小可以分别用Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级来表示，攻击者发起攻击的位置既可以是内部网络，也可以是外部网络，从内部网络发起的攻击称为本地攻击，从外部网络发起的攻击称为远程攻击。还有另外一种攻击的可能性，即伪远程攻击，指系统内部人员从本地获取一些机密信息后，为了掩盖攻击者的身份，攻击过程从外部远程发起，造成外部入侵的假象。为了确定电子政务信息系统安全策略的控制参数，需要明确攻击者的攻击目的。攻击者的目的多种多样，例如政治目的、经济目的、蓄意破坏、竞争等。攻击者发动攻击的可能性及攻击目的的分析如表9.1所示。表9.1中的数据显示，电子政务信息系统要重点防范出于政治目的的间谍从远程或本地发起的攻击，同时要防止内部人员出于经济利益发起的本地攻击或伪远程攻击。另外，蓄意破坏者以纯粹破坏或政治利益为目的发起的远程攻击也不容忽视。

表9.1　攻击者发动攻击的可能性及攻击目的的分析

攻　击　者	攻击可能性			攻击目的			
攻击位置/攻击目的	本地攻击	远程攻击	伪远程攻击	政治	经济	蓄意破坏	竞争
间谍	Ⅱ级	Ⅰ级	Ⅰ级	Ⅰ级	Ⅱ级	Ⅱ级	Ⅱ级
恐怖分子	Ⅳ级	Ⅱ级	Ⅲ级	Ⅰ级	Ⅰ级	Ⅰ级	Ⅳ级
专业罪犯	Ⅳ级	Ⅱ级	Ⅲ级	Ⅳ级	Ⅰ级	Ⅰ级	Ⅳ级
黑客	Ⅲ级	Ⅰ级	Ⅱ级	Ⅲ级	Ⅲ级	Ⅱ级	Ⅳ级
内部人员	Ⅰ级	Ⅱ级	Ⅰ级	Ⅲ级	Ⅰ级	Ⅲ级	Ⅳ级
蓄意破坏者	Ⅱ级	Ⅰ级	Ⅱ级	Ⅰ级	Ⅲ级	Ⅰ级	Ⅳ级

攻击者常常借助一定的工具对电子政务信息系统发起攻击，常用的攻击工具有扫描工具、数据嗅探、木马程序、DoS攻击工具、攻击工具包等，利用这些攻击工具，攻击者可以实现对电子政务信息系统的内外部主机、线路及路由交换节点的入侵。由于信息存储在主机上，电子政务系统应该重点防范对系统内外部主机发起的攻击，适当考虑对网络线路及路由交换节点上的数据嗅探和数据拦截。另外，社会工程攻击已经成为网络攻击中非常流行的入侵方式，社会工程攻击是指利用人们的心理特征骗取用户的信任，获取机密信息、系统设置等不公开资料，从而达到攻击的目的。社会工程学看似只是简单的欺骗，但在信息系统安全中，它的攻击效果是最显著的，其发生的可能性为"Ⅰ级"，因此要高度重视社会工程学攻击方法。

3. 脆弱点分析

在电子政务信息系统的设计、实现、配置及控制过程中，往往存在一些可能被攻击者利用从而造成系统安全危害的漏洞，称为脆弱点。系统中各种资源的脆弱点往往成为攻击者利用的对象，从而实现对电子政务系统的非法或非授权入侵。系统资源包括操作系统资源、数据库资源、公共服务软件、个人工具软件、应用系统、网络管理软件、专用软件、嵌入式软件等。分析电子政务信息系统资源中可能存在的脆弱点发现，由于系统管理员和用户在受教育程度、安全意识方面参差不齐，很难做到系统完全正确的配置，因此由系统配置所产生的脆弱点特别多。同时，由于部分软件厂商在系统安全设计及实施方面缺乏系统、综合的考虑，使得应用系统和专业软件在设计与实现过程中存在"Ⅰ级"安全脆弱点的可能性极大。

另外,电子政务信息系统处理文件资料时广泛采用安全性设计与实现较差的 Microsoft Office 系列的办公软件,因此对于个人工具软件的风险级别也比较高。

4. 支持系统风险分析

电子政务信息系统的支持系统包括通信系统、电力系统、空调系统及消防系统等,这些支持系统的风险主要体现在服务能力的下降甚至是丧失。对于支持系统的漏洞,信息系统应该制定相应的控制机制进行应对。

5. 人员风险分析

工作人员在使用电子政务信息系统过程中,其操作行为可能会给系统带来安全风险,包括人员在业务素质和政治等方面出现的问题。当然,针对这类风险电子政务系统已有相应的控制机制,但人们应该解决从传统的控制机制到网络化的控制机制的过渡。

6. 残余风险分析

任何系统都不可能完全没有风险,并且风险也不可能完全被消除,零风险是不存在的,因此会有一定的残余风险。那些在实现了新的或增强的安全控制措施以后还剩下的风险称为残余风险。残余风险是风险分析的最后一步。完成风险分析并确定风险降低措施后,必须开展进一步的风险评估以保证风险已降至可接受水平。对于电子政务信息系统来说,残余风险若未降低到可接受的水平,那么就必须重复风险管理的过程,直到将残余风险降低到可接受的水平为止。

风险分析的目的是明确安全需求、制定安全规划并实施安全设计,但是由于无法定量地进行风险分析,导致分析结果并不准确,造成了风险分析的局限性。另外,由于攻击手段和方法的不断变化,导致安全风险不可能以穷举的方式对其模式化、固定化。同时,防护机制的投入和产出往往不能准确量化,也会导致风险分析的结果无法准确表达,造成风险分析的困难与缺陷。尽管如此,电子政务系统仍然需要通过风险分析获得将风险控制在可接受范围的方法。

9.1.2 安全需求分析

电子政务系统安全需求分析是进行安全规划与设计的前提和基础。电子政务不同于一般的电子商务,根据我国电子政务建设的现状,系统总的安全需求是安全、保密、可靠、可信。电子政务对安全的特殊需求实际上就是要合理地解决网络开放性与安全性之间的矛盾。在电子政务系统信息畅通的基础上,有效阻止非法访问与攻击对系统的破坏。

用户对系统安全提出的直接且实际的需求是最高层次的安全需求,系统安全的任务就是将用户的这种非专业的实际需求转换成科学合理、专业性的安全需求。从信息保护方式的观点进行分析,可以将用户安全需求分为以下几个方面。

1. Internet 互联需求

电子政务系统与因特网互联,涉及的安全需求包括信息完整性保护、信息源鉴别服务、用户身份识别及访问控制等。根据国家管理机构对电子政务网的相关规定,电子政务网不得与因特网进行物理连接,需要采用物理隔离的方法将二者隔开,从而从根本上防止开放的因特网对政务网构成安全威胁。

2. 内部网互联需求

内部网互联需求包括身份鉴别、访问控制、加密、密钥管理等安全需求。

3. 环境安全需求

电子政务信息系统所处的物理环境(机房、场地设施等)、系统环境(操作系统、数据库系统等)、网络环境(内网与外网)等不受自然、人为等因素破坏的安全需求。同时,环境配置、安全控制及安全培训等也属于环境安全需求。

4. 服务安全需求

电子政务信息系统包含多种服务,例如 Web 服务、电子邮件及各种应用业务等,对应的安全需求即是对这些服务的安全性保障。

5. 功能安全需求

功能安全需求包括对漏洞扫描、入侵检测、身份认证、数字签名、加密解密、访问控制、数据备份与恢复、安全审计、应急响应等功能的安全需求。

6. 性能安全需求

信息系统与安全相关的性能需求有机密性、完整性、可控性、可用性、可审查性及抗抵赖性等。

7. 管理安全需求

电子政务中与管理相关的安全需求包括人员管理、技术管理、系统管理、组织管理、管理开发工具等安全需求。

上述 7 个方面的安全需求分别从不同的角度表达了用户对电子政务信息系统的安全描述。分析上述需求并将其规范化、文档化,最后将规范化的安全需求交由用户进行确认,最终得到电子政务信息系统的正式的、文档化的总体安全需求。

9.1.3　安全规划与设计

以电子政务信息系统的安全风险分析和安全需求为依据,进行安全规划与设计,首先应明确 3 点设计要求:

(1) 对外开放的资源及开放程度。

(2) 要保护的资源及保护程度。

(3) 信息发布及访问的方式。

其次应遵守 8 条设计原则:

(1) 标准化与一致性原则。

电子政务信息系统在进行安全设计时必须遵循一系列的标准和规范,制定明确而前后一致的安全策略和实施过程,从而保证系统的互联互通、信息共享。

(2) 系统安全木桶原则。

系统安全木桶原则是指对信息系统全面、均衡地进行保护。“木桶的最大容积取决于最短的一块木板”。电子政务信息系统是一个复杂的综合系统,它本身在操作、物理和管理上存在种种漏洞构成了系统的安全脆弱性。攻击者肯定会在系统中最薄弱的位置进行攻击。因此,要标识系统安全威胁,评估其脆弱性,及早地检测并汇报最新受到的攻击并采取改进

措施。最后评估安全风险可能造成的损失,以便改进安全机制,优化保护强度。

(3) 整体性原则。

整体性原则要求系统在受到攻击破坏时,能够尽可能快速地恢复工作及服务能力,减少损失。因此,要建立健全系统安全备份与恢复机制,做好应急预案。

(4) 技术与管理相结合的原则。

电子政务信息系统安全涉及人、技术、操作等要素,仅仅依靠管理或技术是不可能实现的。因此,必须将各种安全技术与运行管理机制、操作技能与管理制度培训、安全制度建设相结合。

(5) 统筹规划,分步实施原则。

首先根据网络的实际需求,进行统一规划,建立基本的安全体系,来满足基本的、必须的安全性要求。然后,随着网络规模的扩大及应用的增加,网络复杂度的变化,再加强安全防护力度,并将安全体系逐步细化。

(6) 授权原则。

为电子政务系统中的每种资源设置访问权限,制度访问控制规则阻止对资源的越权使用与操作,对用户进行最小化授权,确定授权用户的职责。

(7) 确认原则。

确认电子政务信息系统中的数据信息的采集、输入、输出、处理、传输及存储等各个环节的安全性、合法性、正确性和有效性。

(8) 成本性能与效能平衡原则。

成本性能与效能平衡原则要求以最小的安全投资成本,取得最大的性能和安全效能。

主要的安全机制和安全技术包括数据加密机制、完整性保护机制、通信保密机制、身份鉴别机制、访问控制机制、网络监控机制、安全审计机制、安全事件响应机制、数据备份与恢复机制、密钥管理机制、防病毒技术、防火墙技术、数字签名技术、网络隔离技术等。

9.1.4 安全解决方案

完整的安全体系结构应覆盖系统的各个层面,包括物理安全、网络安全、系统安全、应用安全及安全管理5个部分。本节从电子政务信息系统的用户及业务需求出发,根据信息系统资源保护的需求,按照信息系统安全体系结构所覆盖的层面,分别从电子政务的物理安全、网络安全、系统安全、应用安全及安全管理5个不同的方面,设计安全解决方案。

1. 物理安全解决方案

电子政务信息系统的物理安全是政务网络系统安全的前提条件。物理安全主要包括环境安全、设备安全和通信线路安全。与此相关的安全标准很多,如《电子计算机场地通用规范》、《计算机场地安全要求》、《信息技术设备的无线电骚扰限值和测量方法》以及国家标准中有关电磁屏蔽的技术标准等。除了遵守以上有关场地安全、防电磁干扰的相关标准外,电子政务信息系统还应该制定严格的机房及信息设备的管理制度,定期分析日志信息,对重要设备配置入侵检测和警报功能,并建立健全重要资源的备份管理制度。

2. 网络安全解决方案

1) 防火墙技术

电子政务系统是一个由省、市、县政府网络组成的三级网络体系结构,从网络安全的角

度来说，它们属于不同的网络安全域，因此在各级电子政务系统的网络边界以及内部网与外部网(如 Internet)之间应采用防火墙技术进行网络隔离，并且要实施相应的安全控制策略。网络边界安全一般采用防火墙等成熟产品和技术实现网络边界的物理隔离，并采用安全检测手段防范非授权用户的入侵或攻击。对外开放查询功能是电子政务系统很重要的一项服务，为了控制关键服务器的授权访问，建议把对外开放的服务器集合起来划分为一个专门的服务器子网，并设置防火墙策略对其进行保护与控制。

2) 漏洞检测及入侵检测技术

为了摆脱被动入侵的境地，电子政务信息系统应该在采取被动防御策略的同时，也启用主动防御功能，漏洞检测及入侵检测技术是主动防御策略的重要组成部分，其目的是提供漏洞的识别与发现、实时入侵检测及采取相应的防护手段，如发现违规行为、内部越权访问、阻断网络连接等行为。

漏洞检测技术通常采用两种策略，即被动式策略和主动式策略。被动式策略是基于主机的检测，对系统中的弱口令、不安全的设置以及其他与安全策略相悖的对象进行检测。主动式策略是基于网络的检测，通过执行一些脚本文件对系统进行攻击，记录系统的反应从而发现其中的漏洞。漏洞检测的结果实际上是对系统安全性能的评估。入侵检测技术大致分为 5 种：基于应用的检测、基于主机的检测、基于网络的检测、基于目标的检测和混合型检测。

不同的网络拓扑结构对漏洞扫描和入侵检测系统功能和结构的要求不同，针对电子政务网络系统，漏洞扫描和入侵检测系统可以设置为安全服务器和检测代理模式，分布在网上的检测代理包括公用服务器检测代理、主机检测代理和网络检测代理。

3) 数据传输安全技术

为了保证电子政务信息系统中各子网之间数据传输的机密性和完整性，同时对用户采用强身份认证，建议在电子政务网中建立安全虚拟专用网(SVPN)，同时采用防火墙技术与密码技术相结合的方法，从而构建安全的内联网。VPN 设备系统为了同时满足电子政务网络安全的通用性和独特性，需要具备以下几个特性：

- 身份唯一性鉴别能力。
- 数据传输加密保证数据机密性、完整性以及抗重放攻击的能力。
- 隧道内明文和密文传输的能力。
- 网络边界隔离及访问控制能力。
- 安全策略、安全体系及密钥的安全管理、配置与审计功能。
- 良好的网络接入透明性。

3. 系统安全解决方案

系统级安全主要包括操作系统安全和数据库系统安全。对于关键的服务器和工作站，如数据库服务器、代理服务器、备份服务器和网管工作站，应该采用服务器版本的操作系统，如 UNIX、Windows Server 等。而对于办公终端、网管终端可采用图形用户界面操作系统。计算机病毒危害严重，为了保护关键服务器及终端设备，必须安装防病毒软件和系统防火墙，并及时更新病毒库，安装补丁程序，关闭不必要的服务。数据库管理系统应该具备自主访问控制、身份验证、授权与审计功能。

4. 应用安全解决方案

电子政务信息系统的应用安全主要处理系统在提供应用业务和服务过程中的安全问题，采用防病毒、身份认证等技术及其他安全措施，对系统所提供的各种应用业务和服务进行安全性配置。

1）典型的应用安全技术

（1）防病毒技术。

病毒是系统中最常见的威胁因素，而病毒防范体系主要解决病毒查杀与清除问题，建立健全病毒防范体系是电子政务信息系统建设的重中之重。根据电子政务的网络系统结构，病毒防范体系由防病毒服务器端和防病毒客户端组成。防病毒服务器端能够实现交互式操作，防病毒客户端进行病毒扫描与查杀，设定病毒防范策略。防病毒客户端安装在系统关键主机中，如关键服务器、工作站和网管终端等。病毒防范体系能够从多个层次进行病毒防范，即在工作站、服务器、网关 3 个层次安装相应的防病毒软件以提供全方位的保护。

（2）身份认证技术。

公钥基础设施对于电子政务实现业务处理具有重要意义。公钥基础设施的存在，为电子政务的事务处理建立信心和信任。公钥基础设施可以做到确认发送方的身份，保证发送方所发信息的机密性、完整性以及不可否认性。

2）应用安全措施

- 实现应用业务运行平台所提供的安全性功能程序与系统所提供的安全性功能程序的互补。
- 在开发应用系统过程中，采用安全服务 API 直接调用或配置某些安全服务模块。
- 根据用户要求重新定制与设备配套的安全应用，如安全电子邮件、网络文件保险柜等。

3）应用安全配置举例

（1）办公自动化平台安全配置。

Lotus Notes 是一个世界领先级的办公自动化工作平台，能够实现迅速、全方位的文件流转、信息采集、处理、查询等应用业务。由于 Lotus Notes 具备一套完善可靠的安全机制，能够提供包括身份认证、数字签名、信息加密解密等安全功能。因此，为了满足电子政务办公自动化应用系统对安全保密的相关需求，可以利用 Lotus Notes 的这些安全功能，对相关应用软件进行修改，实现用户身份鉴别认证、数字签名、访问控制等安全功能，从而极大地提高其安全服务能力。

（2）文件存储安全配置。

文件保险柜是实现电子政务系统中文件的安全存储的一个应用程序，该应用程序的功能不仅可以将文件进行加密保存，还可以提供双因子认证功能。

（3）文件传输安全配置。

在电子政务信息系统中，文件的传输安全是极其重要的，根据文件性质与种类，可分为机密文件、重要文件、关键文件、普通文件、公开文件等，不同种类的文件对传输所要求的安全级别也有差别。但不论是何种文件，在传输过程中都有以下几方面的安全需求。

① 机密性保护：根据文件的种类及其安全要求，对所传输的数据进行不同安全等级的加密保护。

② 完整性保护：数据在传输的过程中不能被篡改。

③ 身份验证：通信双方虽然互不见面，但是要进行通信双方的身份鉴别与验证，以防假冒。

④ 抗抵赖性：文件传输成功后，发送方不能否认其发送的信息，接收方也不能否认其收到的信息，可以通过数字签名实现。

为了实现文件传输的上述安全需求，可以通过文件安全处理程序先对文件进行安全预处理再传送，或者通过安全拨号通信程序来保障传送文件的安全。另外，通过调用安全服务API 修改现有的文件传输程序，也可以提高传输的安全性。

(4) E-mail 安全配置。

E-mail 作为一种非常有效的文件共享和公文传递方法，是电子政务系统使用人数最多、使用频率最高的一个应用软件。使用电子邮件会面临一系列安全问题，例如邮件传递过程中被截获、解读甚至是篡改，同时也会遇到假冒可信任者发送邮件这种非常有害的行为。对于邮件传递过程中的安全问题，可以采用信息压缩、信息加密和信息隐藏等手段来解决。即使邮件被截获，没有密钥的话一样不能解读邮件内容。对于假冒可信者发送邮件这种行为，可以通过数字签名的方法进行邮件收发双方的身份确认，并且还可以防止邮件被篡改。

(5) 信息共享安全配置。

电子政务信息系统将公开信息发布到因特网进行信息共享，以供公众浏览查询，该阶段的基本安全要求是保证信息的完整性和有效性。电子政务系统对外公开的信息多为政策性信息，希望得到公众的广泛关注，这些公开的信息并不需要机密性保护，而需要完整性和准确性的保护。电子政务信息系统内部共享的信息，根据其性质可以分为不同的秘密等级，需要设定相应的访问权限，使得不同级别的用户获得不同的访问授权。CA 认证授权体系为电子政务信息系统的访问授权管理提供了一种较为理想的解决问题的途径。

5. 安全管理解决方案

根据系统风险分析，安全事件的发生在很大程度上是由于系统内部的漏洞以及人为因素，尤其是人员误操作给系统带来严重的损失和后果。虽然通过采取先进的技术措施、引进先进的技术设备可以减少这类安全事件的发生，减少电子政务系统的损失，但是由于系统的主体是人而非技术或设备，人的主观能动性以及复杂性决定了任何先进高级的技术措施或设备都无法取代安全管理在系统安全中的地位。因此，为了维护电子政务信息系统的安全高效运行，降低安全事故发生的可能性，安全管理势在必行。另外，单纯依靠安全管理的手段并不能够完全解决系统所遇到的一切安全问题，从系统辩证法的观点来看，除了应该强调安全管理的重要性以外，还应该采用管理与技术相结合的方法，全面考虑与解决电子政务系统的安全问题。

电子政务信息系统中的系统保护及信息保护需求强度不是仅仅由某一个单位所决定的，而是关系到整个国家的安全需求，是由组织机关根据国家安全需求进行分配与管理的。针对电子政务信息系统，相关的安全管理标准、规范及制度应在国家法律法规和制度的基础上制定。

1) 组织管理

为了加强电子政务信息系统的组织管理，各级党政机关应该建立健全信息系统安全管理机构，并根据国家信息系统安全的相关法律法规和制度规范负责贯彻实施，并完善相关实

施细则。按照垂直管理的原则，电子政务系统的下级机关的安全管理工作由上级机关的安全管理机构进行指导与监督，如果下一级安全管理机构之间发生纠纷和分歧，上一级机构应该肩负起调解与仲裁的责任。安全管理机构的主要职能包括建立系统内部人员的安全操作规程、岗位责任制度，并确定信息系统安全负责人的职能；建立与各级国家信息安全主管机关、技术保卫机构的日常工作关系；严肃处理重大泄密事件、违规及违纪事件。由安全管理机构确定的信息系统安全负责人的职能包括全面负责本单位的信息系统安全工作，组织制定安全教育和培训计划，定期对系统做出安全性评估，管理系统及用户身份识别号码及口令，审查对外公布的信息以防止泄密事件的发生，规范并监督系统操作人员及维修人员的行为，防止信息机密性和完整性受到破坏。

2）人员管理

人员作为电子政务信息系统运行的实施者，既是信息系统安全的主体，也是系统安全管理的对象。加强人员安全管理是确保电子政务信息系统安全的首要任务。

人员管理的对象分为两类：系统管理人员和应用人员。系统管理人员包括系统管理员、安全管理员、安全分析员、关键信息操作员、安全设备操作与维护员、软硬件维修员以及保安人员等；应用人员是使用网络资源完成其本职工作的人员，几乎遍布系统的各个部分。

人员管理的内容涵盖人员审查、岗位分配、人员培训、人员考核、保密合同及人员调离管理。根据电子政务信息系统的安全等级确定人员审查标准，其中最具普遍性的基本素质要求有政治素养高、思想先进、技术合格等。不同岗位的人员分配不同的职责与权限，并设定其完成任务的工作活动范围。关键岗位人选要进行严格的政治、业务能力考核，然后进行必要的政治、技术培训后才允许上岗，并且不能兼任。为保证人员的业务能力和技术水平，需要定期对从事电子政务信息系统的操作及维护人员进行新技术、新知识的培训。对于涉及系统安全设备操作和维护的人员还应该接受安全保密教育与培训。

3）技术安全管理

（1）硬件设备管理。

电子政务信息系统安全运行的重要前提是硬件设备的安全。硬件设备的全方位管理包括硬件设备的购买、使用、保管以及维护等管理行为。

（2）软件管理。

软件管理的范畴涵盖了对操作系统、数据库管理系统、应用软件、工具软件、安全软件和原始数据的采购、安装、使用、更新、维护和防病毒的管理。

（3）密钥管理。

密钥管理原则通常有最小特权原则、最小设备原则、特别分散原则以及不影响系统正常工作原则等。密钥的产生、分发、传送、使用、保存、备份以及销毁等环节都必须遵循安全性设计原则，针对密钥的类型及其生命周期各个环节，采用合适的密钥管理办法，集中生成并管理电子政务信息系统的口令，根据访问权限确定口令的长度并定期更换。

（4）介质管理。

在电子政务信息系统中，介质用于信息的存储、备份等，对信息保护以及系统恢复起到关键作用。因此，应该高度重视介质管理。介质管理的主要内容有介质的使用登记、介质的复制和销毁、介质库、涉密介质以及涉密信息的管理等。

（5）技术文档管理。

技术文档记录了系统在设计、开发及运行维护阶段的所有技术信息，包括系统的构造原理、实现方法、运行维护策略等，为系统的进一步开发与改进提供依据。根据安全级别的不同，技术文档分为绝密级文档、机密级文档、秘密级文档以及一般级文档 4 类。根据密级管理规定，不同密级的技术文档会受到不同级别的安全保护。各级安全管理机构应制定严格的技术文档管理制度，明确管理责任人。在使用技术文档时，要严格履行借阅、复制手续。对于秘密级以上的关键技术文档要进行异地备份。废弃文档的销毁也应该履行严格的销毁、监视制度。

4）防病毒管理

病毒的入侵不仅会影响到信息系统的正常运行，造成严重的经济损失，而且对于电子政务系统来说，病毒侵害甚至还会影响到政治的稳定。仅仅依靠防病毒技术并不能够有效防止病毒侵害，因此为了更好地解决病毒防范问题，必须要加强病毒管理，从管理与技术相结合的角度建立防病毒管理机制。电子政务信息系统的防病毒管理机制必须要依赖先进的病毒防范技术，形成跨平台、多层次、全方位的防病毒工作环境，提供强大的检测、监控以及清除病毒的功能。

防病毒管理机制必须满足如下要求：

- 网络防病毒软件的安装和维护要简便、快捷。
- 客户端防病毒策略要强制定义和执行。
- 病毒识别与扫描机制的更新要方便、集中。
- 发现和处理未知病毒的机制要快速、有效。
- 病毒告警和报告系统管理机制要全面、友好且方便。
- 病毒防护机制服务自动化。
- 防病毒厂商的售后服务与技术支持能力有保证。
- 病毒防范管理机制的建设要维持合理预算。

5）网络连接管理

在电子政务信息系统中，网络连接的方式与情况很多，例如系统要利用公共网络或者直接在公共网络上组建内联网，系统要向公共网络公开发布信息，政府部门会从公共网络上获取信息。

由于电子政务信息系统具有国家性质，因此系统必须要遵循国家安全主管部门关于网络连接的相关规定和要求。即电子政务系统在没有彻底解决安全防护措施之前，必须要将电子政务内部网络与公共网络进行物理隔离。与公共网络连接的计算机网络中不能存放电子政务的敏感信息。

对于利用公共网络组建内部网的电子政务系统，要通过物理隔离的方法将公共网络与内部网络的连接界面分隔开，同时制定相应的访问控制策略。其次，要保障公共网络连接与信息传输的安全，保护信息的机密性与完整性。严禁内部网中的个人计算机通过拨号线路上网。

电子政务系统对外发布的所有信息应及时更新并进行完整性保护，以免影响政府形象，造成政治影响。对外提供的政策性、指导性信息要准确、可靠。严禁系统中的个人绕开管理控制机制直接与公共网络进行信息交换。政府部门从公共网络上获取信息后，必须进行防病毒检测，清除病毒后才可以传送、使用和传播。

6）场地设施安全管理

（1）安全管理标准。

场地设施的安全管理应遵循国家标准《计算机场地安全要求》，该标准将计算机场地设施的安全等级分为A、B、C 3个基本类型。A类对计算机场地的安全有严格的要求，并有一整套完善的安全措施，适合处理秘密级以上信息的场所设施。B类对计算机场地的安全有较严格的要求，有较完善的安全措施，它的安全性介于A类和C类之间，对国家信息系统重要节点运行至关重要的场地设施均要按照B类要求执行。C类对计算机场地的安全有基本的要求，有基本的安全措施，适用于处理其他信息的场地设施。

（2）安全管理要求。

电子政务信息系统的场地设施安全管理必须满足机房场地选择要求，如表9.2所示。

表9.2 电子政务信息系统机房选择安全要求

安全项目	A类	B类	C类
场地选择	⊕	⊕	—
防火	⊕	⊕	⊕
防水	⊙	⊕	—
防静电	⊙	⊕	—
防雷击	⊙	⊕	—
防鼠害	⊕	⊕	—
防辐射	⊕	⊕	—
火灾报警和消防措施	—	⊕	⊕
内部装修	⊙	⊕	—
供配电系统	⊙	⊕	⊕
空调系统	⊙	⊕	⊕

表中符号说明：—表示无要求；⊕表示有要求或增加要求；⊙表示要求与前一级相同。

（3）出入控制。

根据场地设施中信息的安全等级和涉密范围进行分区控制，规定工作人员出入的区域，严格控制各区域和机房的进出口，并根据安全等级和涉密程度设置门卫或电子报警装置，对外部人员访问或者工作人员的跨域访问都要经过安全管理人员的批准并进行登记。

7）应急与恢复

紧急事件发生后，根据事件的类型，采取相应的应急计划与恢复管理，控制系统损失。电子政务信息系统的紧急事件是指已经或将要对系统造成伤害的事件，发生以下任何一种情况，都应视为紧急事件，需要根据应急计划采取相应的紧急措施。

- 破坏性攻击导致系统的硬件或软件不能正常发挥其功能。
- 病毒侵害使系统不能正常工作或工作效率急剧下降。
- 物理设备的人为毁坏导致无法正常工作或工作效率下降。
- 意外停电而后备供电系统不能正常供电。
- 自然灾害的破坏使系统不能正常运行。
- 关键岗位人员擅离职守。

应急计划的内容包括以下5个部分。

- 紧急措施：针对各种类型的紧急事件，制定的响应、救护以及撤离等各项应急措施。
- 资源备份：对软件、电源、大型系统的关键设备和通信及信息安全设备等系统重要资源进行备份。
- 恢复过程：制定并实施灾难发生后的系统恢复过程与步骤，尽可能保证系统受损后能够尽快恢复运行，降低损失。
- 应急计划演习：制定应急计划演习方案并定期进行演习。
- 关键信息：应急计划的关键信息应该张贴在明显的位置，包括报警电话、火警电话以及负责人电话等信息。

应急计划应至少包含两套备用方案，并且每种方案均可独立实施。应急计划应该语言简洁、步骤清楚，责任分工明确，具有较强的可操作性。应急计划流程应该公布在明显的位置，万一事故发生以便应急计划能够得到快速执行。

9.2　金融电子交易系统安全示例

随着信息技术的快速发展，社会信息化程度不断提高，人类社会已经步入一个崭新的时代——信息网络时代。在当前网络日益普及的情况之下，网络金融系统、网络银行、网络证券、电子支付等电子交易系统迅速发展，并得到越来越广泛的应用。

随着电子交易的迅速发展，由于电子交易系统是在公开的网络上进行的，支付等信息和机密的往来文件等大量金融信息在计算机系统存放、传输和处理，电子交易系统的安全已受到来自计算机病毒、电脑黑客、计算机网络系统自身脆弱性等各方面严峻的挑战。所以，交易的安全性是电子交易系统发展的核心和关键问题。

假设有某个大型交易所，虽然用户遍及全国，但是目前仍然采用传统的场内交易方式，大大限制了交易所的发展，因此为了争取更多的用户并为用户提供更加便捷的服务，需要建立网上交易系统。网上交易系统的建立不仅能够提供便捷且无场地时间限制的网络交易，而且还能够扩大用户面以及用户数量。但前提条件是保障用户在网络系统中交易的安全性。电子交易网络系统要实现其金融交易功能，必须要支持场外、场内的交易活动，同时还要提供办公自动化、信息发布以及内部事务管理等服务。网络的开放性特点导致黑客、非法用户以及恶意程序等对电子交易系统的攻击频频出现，所以网络信息安全成为交易网络系统得以稳定高效运行的重要保障。因此，需要建立一整套交易系统安全体系结构来保障网络交易系统本身以及业务系统、信息传输和存储安全。

9.2.1　安全风险分析

1. 系统资产识别

金融电子交易系统的资产主要包括硬件资产、软件资产、用户资产以及信息资产等。

电子交易整个网络系统中以及网络外围的硬件设备都属于硬件资产，包括个人计算机、服务器、网络设备、安全设备、传输介质、终端、输入输出设备、电源、打印机等。依赖于以上所有硬件资产而运行的软件产品都称为软件资产，目前主要识别出的软件资产有操作系统、数据库管理系统、网络管理软件、Internet 公共服务软件、专用软件等。系统外以及系统内

的各种安全风险和威胁都可能会对软硬件资产造成影响。由于软件资产以及数据信息对硬件的依赖性，所以硬件资产的任何风险都可能会影响到电子交易系统安全。由于信息资产的传输、存储和处理过程均要有软件资产的参与，因此软件资产面临的风险也将会影响到系统安全。

用户是确保电子交易系统安全的关键环节，系统用户资产由网络交易员、系统业务员、系统管理员、系统维护员组成。实际上，一部分安全事故的发生是由于用户的操作不当所致。因此提高用户安全意识、改善用户操作习惯可以有效降低用户给系统带来的安全隐患。而确保用户安全的根本措施是设计完善的权限控制和访问控制体系。

电子交易系统的核心是信息资产，在交易网络中存在各种各样的信息资产，其中交易性信息资产、办公业务及管理信息资产是两类最常见、最重要的信息资产。交易性信息资产涵盖了网络交易过程中产生的各种实时和历史交易信息、发布的数据信息和各种管理文档等。办公业务及管理信息包括系统配置信息、安全管理信息、审计与监控信息以及用户使用的各类敏感信息。在信息资产识别过程中，为了便于后续的风险分析，应该根据信息资产的价值对其进行敏感度划分。一旦受到威胁，应该首先保护敏感度高的信息。

(1) 敏感信息。只对交易人员本人或系统一定范围的人员开放。从用户身份认证、访问控制到交易数据交换处理等环节，针对敏感信息尤其是远程交易的数据信息，都要进行严格的机密性和完整性保护。

(2) 内部信息。仅对系统内部部分或全体人员开放的信息。内部信息需要进行授权访问并对信息的机密性和完整性进行合理保护。

(3) 公共信息。对系统内外部人员都开放的一类信息。所有人都可以进行浏览和获取。为确保使用者能够及时准确地获取所需的信息，系统必须保证公共信息的完整性和有效性。

2. 系统风险分析

1) 一般性风险分析

通常金融电子交易系统所面临的一般性风险就是安全攻击。攻击分为两种：主动攻击和被动攻击。

主动攻击可以是来自于系统内外部的人员主动入侵系统，影响或改变系统的运行状态，导致系统不能够正常工作甚至是系统瘫痪。主动攻击会给电子交易网络带来灾难性的损失和后果。主动攻击的形式大体包括：

(1) 入侵。利用网络或系统的漏洞侵入系统并进行非法复制、更改数据，甚至获得系统管理特权从而操纵系统资源等。系统内部人员如管理员或操作员等本来就具有进行系统操作资源的权限，因此很容易进行攻击。防御不严的网络系统也极易引来黑客的入侵。

(2) 假冒。预先获得合法用户的身份标识或权限以后，攻击者会假冒合法用户的身份行使其权限，比较严重的情况是假冒系统管理员进行操作。

(3) 重放。攻击者利用网络监听或其他方式盗取合法、正常的认证交互信息，然后将其重新发送给认证服务器，从而达到欺骗系统的目的。重放攻击是黑客常用的攻击方式。

(4) 篡改。攻击者在获取系统中文件、数据等信息资源的存取权限以后，执行修改、删除或添加等破坏性操作的行为称为篡改，被篡改的信息的完整性和机密性均受到严重破坏。

(5) 抵赖。某行为实体对已经发送或接收信息的行为进行事后抵赖，造成责任混乱，因此也称为否认型攻击。也就是说，某行为实体对自己发出或接收信息的行为有预谋地或故

意地不负责任、进行否认或抵赖。抵赖型攻击是电子商务中的重大安全问题之一。可以采用数字签名、身份认证等技术措施来防止和抵抗抵赖行为。

(6) 病毒攻击。向系统注入能够进行自我复制的病毒程序,病毒运行后可能损坏数据甚至造成系统瘫痪。

被动攻击主要是收集信息而不是进行访问,更不会改变数据资源以及系统的运行状态,但会盗用信息资源并用于非法目的。攻击可以来自网络系统的内部或外部。被动攻击的形式包括信息窃取、密码分析以及通信流量和流向分析。

(1) 信息窃取。攻击者从传输信道、存储介质等处窃取信息,如搭线监听、无线传输信号侦收、窃取数据文件或直接进行数据复制等。

(2) 密码分析。对截获的已加密信息进行密码破译,从中获取有价值的信息。

(3) 通信流量和流向分析。对网络传输中的信息流量和流向进行分析,然后导出有价值的信息,从而为组织系统的攻击收集资料。

2) 电子交易系统风险分析

电子交易系统的安全风险可以说是来自于方方面面,既包括主动和被动攻击所带来的威胁,也包括管理不善带来的风险。主动威胁可以是网络资源拒绝服务攻击,造成系统资源对系统降低甚至是丧失正常服务能力,也包含了信息篡改与重放、恶意程序攻击、假冒合法用户、伪造合法系统服务等一系列威胁。被动威胁的手段有截获用户数、密码分析、信息流和信息流向分析等。由管理不善所带来的风险更是多种多样。对系统内部人员和用户的行为管理不善可能会给系统带来风险。一旦系统管理员操作或决策失误就一定会带来系统风险,如果管理员未按规定启动系统安全保护体系以及关键性的系统组件,系统的安全防御能力就会降低,甚至会面临体系崩溃的风险。无论是非授权用户非法使用系统资源,还是授权用户越权使用资源,以及系统的授权信息的互相转让,均可能造成资源的滥用和误用,甚至会破坏系统运行。缺乏对系统环境的管理,不重视系统物理环境中脆弱性的识别与改进,会给不法分子窃取以及破坏物理网络硬件资产等攻击行为带来可乘之机。

9.2.2　安全需求分析

金融电子交易系统的安全需求主要体现在两个方面:一方面是交易系统内部应用业务和管理系统的安全保障;另一方面是交易系统通过 Internet 进行数据传输、处理、存储以及远程交易业务的安全保护需求。

1) 系统内部安全保障

在金融电子交易系统内部,具有安全保障需求的资源包括内部网络管理系统、管理信息系统、各部门业务系统以及交易所大楼接入系统等。通过对系统内部资源进行分析,电子交易系统内部主要的安全保障需求包括:

(1) 系统隔离。在交易系统与 Internet 的网络接入点位置,需要通过安全可靠的物理隔离或逻辑隔离设备及手段将系统交易区域与内部网络区域隔离开,系统用户区域和网络资源区域之间也不能够直接连通,必须进行系统隔离。另外,对于局域网中应用业务系统和交易系统中重要资源的网段之间也必须要进行物理隔离或 VLAN 划分。

(2) 数据加密。对于交易系统内部保存和传输的且与交易和管理有关的所有数据信息,都要进行敏感数据的加密存储和加密传输。

(3) 身份认证。身份认证是确认实体身份真实性的过程,包括鉴别与认证两个环节,是实施访问控制的前提条件。

(4) 访问控制。用户请求访问交易系统资源及交易数据时,进行的基于身份和权限的控制过程,包括认证与授权两个环节。

(5) 抗抵赖。为了实现交易的不可否认性,必须建立抗抵赖体系,为交易系统之间以及系统内外部之间的抵赖行为提供证据和仲裁服务。

2) 与 Internet 连接的安全需求

系统与 Internet 的连接存在一系列的风险与威胁,但是交易系统必须要通过 Internet 进行数据传输、处理、存储以及远程交易业务。在进行网上交易过程中,为了降低风险事件发生的概率,我们对交易系统提出以下几点安全保护需求。

(1) 系统管理员安全要求。

系统管理员首先应具备管理系统的业务能力和道德、政治素质,不能滥用或转让权限,遵守安全策略与操作规程,其操作行为必须经过认证、授权并对自己的行为负责,及时地进行系统的日常维护和病毒清理,不能损害系统输入输出数据。

(2) 系统运行及通信要求。

由于系统的软硬件环境是保障交易系统安全可靠稳定运行的关键,用户不能随便移动或修改系统硬件、程序、数据或日志文件。系统通信过程中应该对通信线路进行物理保护,以防止未授权的物理访问或者恶意破坏。

(3) 口令文件保护需求。

为了妥善保护系统口令文件,除了系统授权的情况以外,任何用户不得对口令文件进行访问或修改。

(4) 对抗攻击能力。

系统应具备一定的对抗攻击的能力,确保外部人员无法捕获及识别通信线路中传输的数据,并制定完善的应急响应计划以及系统恢复过程。

(5) 系统容灾与恢复能力。

系统能够对抗自然灾害及人为危害的能力,并对关键资源进行备份,如备用电源、备用通信线路等,保证系统某一个部分发生故障时,系统的运行和服务能够尽快恢复。

9.2.3 安全规划与设计

交易系统的安全规划与设计总体方案的确定需要参照安全设计的原则,并结合电子交易的相关业务,制定相应的安全设计目标,从而构建详细的安全体系。

1) 安全设计原则

(1) 统筹规划,分步实施。

详细分析电子交易系统所面临的各方面风险与威胁,有针对性地建立网上交易系统的基本安全体系架构,并采取分步实施的原则,逐步实现关键业务以及交易网络的整体安全。

(2) 投入与效益平衡。

在不降低系统网络效率的前提下,以适当的安全投入,获得适度的网络安全效益。

(3) 可用性。

安全的最终目的是保障交易系统的正常、有序、稳定的运行。因此,必须要在资源可用

性的基础上，尽可能地不影响网络的结构以及系统应用业务的正常运行。

(4) 可扩展性。

为了适应日后用户量逐渐增加的发展趋势，安全设计和实施必须能够支持应用业务系统的功能扩展需求，同时也能限制交易网络规模的拓展变化以及升级换代。

2) 安全设计目标

运用先进的技术和产品，建立安全可靠、稳定运行的网上交易系统是安全设计的总体目标。网上交易系统应该具备完善的安全保障体系，支持各种网络交易活动，并且不限制系统的扩展需求。网上交易系统的安全设计目标如下：

(1) 交易系统的传输和存储安全以及运行安全得到有效改进，系统抗风险能力得到显著提高。

(2) 采用安全措施对交易所局域网进行从网络划分、系统设置到子网隔离等多方面的安全性改造，使得局域网的抗风险能力得到明显提升。

(3) 对交易所综合业务系统中数据安全传输、存储、身份认证以及网络业务等方面进行安全性改造，保障敏感信息的机密性和完整性。

9.2.4　电子交易系统安全体系

根据安全风险和安全需求分析结果来确定电子交易系统的安全体系及安全策略，合理配置系统中的安全机制、安全服务以及安全管理等各个模块。根据金融电子交易系统的实际安全需求，从网上交易安全、应用业务安全、网络系统安全、关键信息加密等安全技术方面以及安全管理方面进行安全体系设计与构建。

1. 网上交易安全

根据电子交易系统的特点，网上交易安全可以通过两种方式来实现。

1) 代理公司独立管理方式

该方式是由系统交易中心授权给各代理公司，然后由代理公司来处理用户的交易业务，实现网上交易的安全。交易业务的受理是在代理公司进行，而不是在电子交易系统内部执行。

在代理公司独立管理方式下，交易系统的安全解决方案是通过在各代理公司配置安全服务器、审计服务器、证书管理中心以及用户端密码机等系统安全设备来实现的。这种设计方式主要实现的安全服务功能包括身份认证、数据加密、数据传输安全处理、安全隔离以及安全审计等。用户可以通过两种方式在交易系统开户：一种是在代理公司开户，代理公司所属的发卡中心负责这类用户的开户管理；另一种是在交易中心直接开户，用户开户后，交易中心的发卡中心会直接对用户进行开户管理。成功开户的用户会获得存储着个人私钥信息的用户身份卡，该卡可以确保用户敏感信息的安全存储以及不可复制。当系统用户数量以及业务量显著增加的时候，在现有的管理方式下，代理公司交易系统的规模已经无法适应当前的交易业务需求，因此要对网络系统进行扩展或升级。在考虑不影响网络拓扑结构的前提下，增加各代理公司的安全服务器以及桌面密码机的数量，可以有效解决扩大后的交易业务需求，而且也不会因为用户点的增多而改动网络系统结构。

在代理公司独立管理方式下，交易系统通过 Internet 进行网上交易的安全问题由代理公司负责解决。在交易中心进行的交易，代理公司只实现用户的身份认证过程，然后将信息

交由交易中心处理,交易中心根据其安全配置负责网上交易的安全。在代理公司进行的交易,其网上交易安全可以通过代理公司的安全服务器以及客户端桌面密码机来实现。

2）系统统一管理方式

该方式由系统交易中心统一进行交易业务的处理与管理,是比较直接的实现方式。由于系统统一管理,所有通过 Internet 进行网上交易的业务都在交易中心接入。交易中心负责用户的网上交易安全问题。用户进行网上交易时必须使用配有桌面密码机装置的客户端,用户通过客户端向中心服务器发送访问请求,请求由安全交易受理机处理,受理过程中的安全策略由服务器和业务系统提供,从而实现安全的网上交易过程。

2. 局域网安全

交易系统的局域网安全设计要同时考虑 3 个方面:网络隔离、访问控制以及加密传输。首先要利用防火墙技术,对局域网与公共网络的边界进行网络隔离及访问控制,有效防止公共网络的安全风险威胁到交易系统内部网络。其次,局域网中网络资源和用户群要通过网段隔离(子网划分)的方式加以分割。在进行敏感信息传输的过程中,使用加密隧道技术保障子网间的数据通信与传输的安全。

电子交易系统的网络划分方式多种多样。例如,根据网络资源的种类、用户类型以及业务类型的不同,可以采用网络划分技术实现网络资源与用户的隔离。又如,根据交易网络中资源的敏感程度划分为普通信息网和敏感信息网,并将二者进行物理隔离,针对敏感信息网实施安全策略,防止非授权用户的非法访问,保障网络系统的整体安全性。另外,按照系统机构设置可将交易系统划分为业务主网和若干个业务子网,从而控制业务主网与业务子网、业务子网之间的信息流向。

交易系统局域网的访问控制需要实现管理信息流向、过滤风险连接与服务的功能,可以通过防火墙或具有防火墙功能的 VPN 设备实现。当用户请求访问局域网中相关网络资源时,防火墙或 VPN 设备首先要对用户名、账号与口令进行识别与验证,从而对用户的身份进行鉴别,只有通过身份鉴别的用户才可以访问请求的资源,同时防火墙或 VPN 设备还要控制用户的访问时间、可访问的资源类型以及访问权限等。另外,系统管理员负责用户账号的建立与维护,并控制和限制用户的账号使用、网络访问时间与访问方式。

3. 应用系统安全

交易网络中的应用业务系统主要包括场内交易系统、办公自动化系统、部门业务处理系统、管理信息系统等。

场内交易系统在处理所有用户敏感信息时,首先要对用户身份进行识别与验证,进而控制其操作权限;其次,场内交易系统处理的所有敏感信息的传输都必须经过加密处理,从而确保数据在传输过程中不被窃取或篡改。

利用 Lotus Notes 平台提供的访问控制、远程传输等功能,修改相关应用业务软件,即可获得身份认证、数字签名、加密传输等安全服务功能,从而保证办公自动化系统的安全。

交易系统以及办公自动化系统中保存着大量的敏感信息,加密存储是解决敏感信息存储安全的最好方法,文件的加密存储方式有嵌入式文件加密系统方式和加密系统外挂方式。

交易系统对内部和外部都会提供信息浏览、查询等服务,保证这些信息服务的基本安全措施有数据源鉴别服务、数据机密性服务、数据完整性服务、抗抵赖服务、访问控制服务等。

4. 应用业务安全

在交易业务受理过程中，如何防止用户信息的非法访问与篡改，有效保护用户的交易信息是电子交易系统安全的关键。在交易过程中，为了保护应用业务数据的机密性、完整性以及对数据的访问控制，可以根据代理公司的业务量大小，选用信息加密、数字签名和身份认证等技术措施。这里建议配置金融数据加密机来解决应用业务安全问题。该加密机是以现代密码技术为核心的主机安全模块，是一个具有物理安全保护措施的硬件设备，具有自主密钥管理机制，能将密码运算过程封装在内部完成，从而为主机提供安全的应用层密码服务，如密钥管理、消息验证、数据加密、签名的产生和验证等密码服务，保证数据从产生、传输、接收到处理整个过程的安全性、有效性、完整性、不可抵赖性等安全问题。

在网络交易中心，由于业务量较大，一般要求配备级别比较高的 A 型金融数据加密机。由于交易中心需要处理多个代理公司的业务数据，为了满足业务处理能力，金融数据加密机的加密、数字签名以及验证的速度要足够快。

在各代理公司，由于其用户量以及应用业务量较少，因此在代理公司业务处理中可以选择配置性能较低的 B 型或 C 型金融数据加密机。当代理公司将数据传送到交易中心时，代理公司的业务数据的加密、数字签名以及身份认证等环节首先要由 B 型或 C 型金融数据加密机进行处理，然后传送到交易中心的业务主机，再由 A 型金融数据加密机进行数据的加解密和验证处理。

由于各型的金融数据加密机能够提供多种速率、多种类型以及多种标准的通信能力，并且都使用同一种加密算法，因此可以保证业务数据在整个网络传输、处理以及存储过程中的完整性、机密性以及可用性。

5. 安全管理

安全体系设计包括两个方面：主动防御体系和被动防御体系。主动防御涉及系统扫描检测、入侵检测、跟踪、告警、安全审计等安全策略。安全管理属于主动防御范畴。除了以上安全措施以外，安全管理还涉及对信息系统及其运行环境的法律约束、安全管理制度、组织管理以及人员管理等。

1）软硬件安全管理

软硬件安全管理所要达到的目标是保证交易网络系统中的软硬件实体具有一个良好的运行环境。

需要进行管理的硬件设备主要有服务器和客户机、通信设备以及网络设备等，硬件设备运行环境应该能够防自然灾害（如抗电磁辐射、防火、防水、防雷电等）和人为灾害（如防移动、盗取和破坏等）。硬件安全管理措施包括门禁保护、监控与告警等。

需要进行管理的软件包括支撑软件和应用软件两类。主要的支撑软件有操作系统、数据库软件、开发工具软件等，对于操作系统而言，一般需要进行的安全管理与维护工作包括：

- 定期整理文件系统。
- 监控服务器的活动状态和用户注册数。
- 定期清理日志文件、临时文件。
- 处理运行中的死机状况。

应用软件的管理和维护主要是版本控制，为了保持客户机上的软件版本一致，应该设置

一台安装服务器，当远程客户机应用软件需要更新时，就可以从网络上进行远程安装。

软硬件的安全管理与维护还应该做好数据的备份与恢复工作。利用多种介质，如磁介质、纸介质、光盘、硬盘等，对系统数据进行存储、备份和恢复。这种安全保护措施包括对系统设备的备份、关键数据的备份、重要系统的备份等。

2）病毒的安全防范管理

病毒的安全防范应该从技术和管理两个方面同时进行，从技术角度考虑，交易系统服务器端和客户主机上应该安装防病毒软件，进行病毒检测、清除以及免疫，并定期更新防病毒软件和病毒库。在管理上应该制定一整套规章制度，如不能擅自从网络上下载软件并使用，以防软件中隐藏的病毒对交易系统构成威胁。

3）人员安全管理

人员安全管理的主要任务是提高有关人员的安全意识，严格选拔业务管理人员并落实工作责任制。人员安全管理的对象包括安全管理人员、系统管理人员、保安人员以及用户。人员管理安全运转一般要遵循以下基本原则：

- 最小特权原则。
- 双人负责原则。
- 任期有限原则。

4）保密管理

金融电子交易系统涉及各方面的机密信息，需要划分信息的安全级别，确定安全防范重点，提出相应的保密措施。信息的安全级别一般分为3级：绝密级、机密级、秘密级。绝密级信息不允许在互联网上公开，仅限于高层管理人员掌握。机密级信息也不允许在互联网上公开，只限于中层以上管理人员使用。秘密级信息可以供用户浏览，但是必须设置保护程序，以防黑客入侵。

5）系统安全审计

系统安全审计的主要工作是收集并分析交易系统中所有业务活动的日志记录、违规记录和入侵检测信息等，从而发现并追踪系统的非法活动，降低系统运行的风险。系统安全审计是电子交易系统安全体系结构的重要组成部分。

安全审计专用设备（如审计监控服务器）以及安全设备（如防火墙）都能够为电子交易系统提供安全审计服务。对于操作系统、数据库管理系统的安全审计可以通过审计监控服务器实现。网络边界以及网络通信的安全审计可通过防火墙等安全设备所提供的审计功能负责实现。根据应用业务交易情况以及业务软件的日志信息，可用安全管理软件对其进行安全审计。

9.3 本章小结

本章介绍了两种典型的信息系统的安全示例，电子政务信息系统和金融电子交易系统，并分别提出了详细的安全解决方案，包括系统的安全风险分析、安全需求分析、安全规划与设计等过程，为电子政务信息系统和金融电子交易系统的全面安全及其使用该系统的组织或机构提供一套安全可靠的参考解决方案。

9.4　习　　题

1. 电子政务系统的安全需求包括哪些?
2. 电子政务系统的安全风险包括哪些?
3. 如何确保电子政务系统的安全或简述电子政务系统的安全解决方案。
4. 简述金融电子交易系统面临的安全威胁或风险。
5. 假设某公司有一个信息管理系统,简要叙述该如何设计其安全解决方案。

参考文献

[1] 关义章,戴宗坤,罗万伯等. 信息系统安全工程学. 北京：电子工业出版社,2002.12

[2] 戴宗坤,罗万伯. 信息系统安全. 北京：电子工业出版社,2002.11

[3] 戴宗坤,罗万伯,唐三平等. 信息系统安全. 北京：金城出版社,2000.3

[4] 赵俊阁,陈泽茂,薛丽敏等. 信息安全工程. 武汉：武汉大学出版社,2008.9

[5] 沈昌祥. 信息安全导论. 北京：电子工业出版社,2009.12

[6] 沈昌祥. 信息安全工程导论.北京：电子工业出版社,2003.7

[7] 张基温. 信息系统安全教程. 北京：清华大学出版社,2007.7

[8] 石文昌,梁朝晖. 信息系统安全概论. 北京：电子工业出版社,2009.3

[9] 杨孔雨,郁红英,王晓敏. 信息系统基础. 北京：清华大学出版社,2010.10

[10] 陈运. 信息论与编码. 北京：电子工业出版社,2007.9

[11] 罗森林. 信息系统安全与对抗技术. 北京：北京理工出版社,2005.8

[12] 胡爱群,宋宇波,蒋睿. 信息安全. 武汉：华中科技大学出版社,2011.1

[13] 洪帆,汤学明,崔永泉等. 访问控制概论. 武汉：华中科技大学出版社,2010.

[14] 中国信息安全产品测评认证中心. 信息安全理论与技术. 北京：人民邮电出版社,2003.9

[15] 林东岱,曹天杰等. 企业信息系统安全：威胁与对策. 北京：电子工业出版社,2004.1

[16] 曹阳. 基于三视图框架的分布式信息系统安全体系结构研究[博士学位论文]. 国防科学技术大学,2002.10

[17] 张红旗,王新昌,杨英杰等. 信息安全管理. 北京：人民邮电出版社,2007.11

[18] 钱钢. 信息系统安全管理. 南京：东南大学出版社,2004.10

[19] 张基温. 信息系统安全原理. 北京：中国水利水电出版社,2005.1

[20] 冯登国. 信息社会的守护神：信息安全. 北京：电子工业出版社,2009.9

[21] 范红. 信息安全风险评估规范国家标准理解与实施. 北京：中国标准出版社,2008.2

[22] 吴亚非,李新友,禄凯. 信息安全风险评估. 北京：清华大学出版社,2007.4

[23] 王英梅,王胜开,陈国顺等. 信息安全风险评估. 北京：电子工业出版社,2007.6

[24] 赵战生,谢宗晓. 信息安全风险评估——概念、方法和实践. 北京：中国标准出版社,2007.8

[25] GB/T 20984-2007.信息安全技术信息安全风险评估规范,2007. 6

[26] 何鑫,郑军,刘畅. 软件安全性测试研究综述. 计算机测量与控制,2011.3

[27] 陈璇. 浅谈关于软件安全性测试方法研究. 电脑知识与技术,2009.3

[28] 施寅生,邓世伟,谷天阳. 软件安全性测试方法与工具. 计算机工程与设计,2008.1

[29] 施寅生,邓世伟,谷天阳. 软件安全性测试方法研究. 微型计算机,2008.1

[30] 吕金和. 软件安全性测试研究. 计算机安全,2010.8

[31] GB/T 25070-2010.信息安全技术——信息系统等级保护安全设计技术要求, 2010.9

[32] GB/T 25058-2010.信息安全技术——信息系统安全等级保护实施指南, 2010.9

[33] GB/Z 24364-2009.信息安全技术——信息安全风险管理指南,2009.9

[34] 邝孔武,王晓敏. 信息系统分析与设计. 北京：清华大学出版社,2006.4

[35] 张焕国,崔竞松,王丽娜. ISSE在信息系统中的应用. 计算机工程,2003.11

[36] 陈海燕译. An Introduction to Computer Security：The NIST Handbook（NIST SP 800-12）中文版 V1.00. 1995.10

[37] 微软安全风险管理指南. 2004.12

[38] 王兴芬,李一军. 信息系统安全工程概念与方法研究. 合肥工业大学学报(自然科学版),2003.8
[39] 付钰,吴晓平,王甲生. 基于模糊—组合神经网络的信息系统安全风险评估. 海军工程大学学报,2010.2
[40] 王利,贺静,张晖. 物联网的安全威胁及需求分析. 信息技术与标准化,2011.5
[41] 张一新. 网络信息安全风险及需求分析. 水利水电技术,2007.5
[42] 陈军,薄明霞,王渭清. 云安全需求分析及解决方案初探. 电信科学,2011.10
[43] 曹阳,张维明. 信息系统安全需求分析方法研究. 计算机科学,2003.4
[44] 赵卫东. 信息系统生命周期中的安全工程活动研究. 计算机工程与科学,2004.12
[45] 张灼,张勇. 信息系统安全与风险管理之我见. 网络与通信,2009.3
[46] 赵力. 风险评估与安全需求的关系. 信息安全与通信保密,2004.11
[47] 曾芷德. 数字系统测试与可测试性. 湖南:国防科技大学出版社,1992.12
[48] 颜炯,王戟,陈火旺. 基于模型的软件测试综述. 计算机科学,2004.2
[49] 刘守澜,卿昱. 信息系统安全风险评估方法的研究. 西南民族大学学报自然科学版,2010.2
[50] 罗衡峰,杨晓明,张利. 信息系统安全风险评估综述. 电子产品可靠性与环境试验,2008.4
[51] 吴敬,赵冬梅. 信息系统安全风险评估定量方法比较研究. 电脑知识与技术,2011.3
[52] 崔健双,李铁克. 网络信息系统安全研究现状及热点分析. 计算机工程与应用,2003.9
[53] 李鹤田,刘云,何德全. 信息系统安全风险评估研究综述. 中国安全科学学报,2006.1
[54] 谭兴烈,周明天,沈昌祥. ISSE 在安全系统设计中的应用. 计算机科学,2003.3
[55] 程秀权. 信息系统安全规划框架与方法. 现代电信科技,2007.6
[56] 方勇,刘嘉勇等. 信息系统安全导论. 北京:电子工业出版社,2003.3
[57] (美) Sari Stern Greene. 安全策略与规程原理与实践. 陈宗斌等译. 北京:清华大学出版社,2008.10
[58] 洪翔,江建慧,吴瀛等. 轨道交通企业信息系统的安全规划. 计算机应用与软件,2010.6
[59] 孙大奇. 一种信息系统的安全规划与评估方法. 信息安全与通信保密,2001.4
[60] 陆宝华,王楠. 信息系统安全原理与应用. 北京:清华大学出版社,2007.11
[61] 计金玲. 信息系统建设规划与管理中的安全策略. 计算机安全,2010.11
[62] 于慧龙. 大型企业信息系统安全建设总体规划的建议. 计算机安全,2004.9
[63] 胡传兵,蔡红柳,何新华等. 基于企业信息系统安全模型的构建与实现. 计算机工程,2004.7
[64] Nicholas L Norfolk. An Investigation of the Design and Implementation Flows of Information Systems Security Models. Region 5 Technical Conference. IEEE, 2007.4
[65] 黄益民,平玲娣,潘雪增. 信息安全模型的研究及安全系统方案设计. 浙江大学学报(工学版),2001.11
[66] 蒋韬,李信满,刘积仁. 信息安全模型研究. 小型微型计算机系统,2000.10
[67] 郑晓妹. 信息系统安全模型分析. 安徽科技学院学报,2006.1
[68] 何建波,卿斯汉,王超. 对两个改进的 BLP 模型的分析. 软件学报,2007.6
[69] 刘彦明,董庆宽,李小平. BLP 模型的完整性增强研究. 通信学报,2010.2
[70] Wei Ou, Xiaofeng Wang, Wenbao Han, etc. Research on Trusted Network Model Based on BLP Model. 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009.11
[71] 唐成华,陈新度,何圣华. C/S 模式信息系统的安全性控制策略. 微机发展,2003.8
[72] 张守伟,宋文爱. 基于 B/S 模式的管理信息系统安全问题研究. 黑龙江科技信息,2008.2
[73] 何绍华,王亮. 网络信息系统中信息保护的实现. 图书情报知识,2003.2
[74] Yihe Liu, Xingshu Chen. A NEW INFORMATION SECURITY MODEL BASED ON BLP MODEL AND BLBA MODEL. ICSP' 04 Proceedings. IEEE,2004.9
[75] 雷新锋,刘军,肖军模. Chinese Wall 模型在开放综合安全模型中的实现. 北京邮电大学学报,

2009.6
[76] 李建华. 信息系统安全管理理论及应用. 北京：机械工业出版社，2009
[77] 江常青，邹琪，林家骏. 信息系统安全测试框架. 计算机工程，2008.1
[78] 温熙森，胡政，易晓山等. 可测试性技术的现状与未来. 测控技术，2000.1
[79] 康中尉. 可测试性设计研究. 微计算机信息，2008.1
[80] 刘剑. 软件可测试性检测技术研究与实现. 南京航空航天大学，2004.1
[81] 刘菲菲，赵怀勋，祁冰. 软件可测试性分析方法的研究. 现代电子技术，2003.12
[82] 钱红兵，赵巍，程杜平. 软件可测试性检测技术研究. 计算机应用，2004.4
[83] 于洁，杨海燕，高仲仪等. 软件的可测试性设计. 计算机工程与应用，2003.1
[84] 王坤. 软件可测试性检测系统设计与实现. 福建电脑，2008.10
[85] 范灵春，眭俊华. 软件可测性度量研究. 计算机工程与设计，2006.11
[86] 付剑平，陆民燕. 软件测试性设计综述. 计算机应用，2008.11
[87] Haiyan Liu，Yuwen Cheng，Zhaohong Yang，Zhanjun Zhang. Research on Security Testing of Information System Based on Interface Communication[J]. IEEE，2011.8
[88] Mehrdad Majzoobi，Farinaz Koushanfar，Miodrag Potkonjak. Testing Techniques for Hardware Security[J]. IEEE，2008.10
[89] Nachiketh Potlapally. Hardware Security in Practice：Challenges and Opportunities[J]. IEEE，2011.6
[90] Farinaz Koushanfar，Miodrag Potkonjak. Hardware Security：Preparing Students for the Next Design Frontier[J]. IEEE，2007.6
[91] Alexander Adamov，Vladimir Hahanov. Security Risks in Hardware：Implementation and Detection Problem[J]. IEEE，2010.9
[92] Alain MERLE，Jessy CLEDIERE. Security testing for hardware products：the security evaluations practice[J]. IEEE，2005.7
[93] 余亚玲，唐红武，杜海霞. 基于日志的安全事件管理系统的研究与实现. 计算机工程，2007.8
[94] 杨峰，段海新，李星. 一种协同式安全事件处理系统. 计算机工程，2003.11
[95] Michael A. Harper. A SYSTEMS ENGINEERING METHODOLOGY FOR THE DEVELOPMENT OF DISASTER TOLERANT COMPUTER AND COMMUNICATION SYSTEMS[博士论文]. School of Engineering Southern Methodist University，2009.5
[96](美)Jon William Toigo. 灾难恢复规划(第三版). 连一峰，庞南等译. 北京：电子工业出版社，2004.5
[97] 王琨，周利华，袁峰. 信息系统灾难恢复模型研究. 计算机应用，2006.6
[98] 王琨，尹忠海，周利华等. 信息系统灾难恢复计划研究. 电子与信息学报，2007.4
[99] 王琨，尹忠海，周利华等. 基于最优化理论的灾难恢复计划的量化数学模型. 吉林大学学报（工学版），2007.1
[100] Hongyang Zhang，Lihong Zhao. Data Security in Disaster Recovery System. 2010 International Conference on Computer Application and System Modeling（ICCASM 2010），2010.10
[101] 张艳，李舟军，何德全. 灾难备份和恢复技术的现状与发展. 计算机工程与科学，2005.2
[102] 劳眷. 灾难备份和恢复技术及解决方案分析. 计算机应用与软件，2005.3
[103] 刘涛，刘晓洁，曾金全等. 信息系统容灾抗毁原理与应用. 北京：人民邮电出版社，2007.10
[104] 中国信息安全测评中心编著. 信息系统灾难恢复基础. 北京：航空工业出版社，2009.6
[105] 彭友，王延章. 信息系统内部安全审计机制. 北京交通大学学报，2009.4
[106] 韦勇，连一峰. 基于日志审计与性能修正算法的网络安全态势评估模型. 计算机学报，2009.4
[107] 王景中，徐小青. 计算机通信信息安全技术. 北京：清华大学出版社，2006.3
[108] 胡美新，王小玲. 安全审计技术在计算机系统中的应用研究. 湖南科技学院学报，2007.9
[109] 杨仁华，刘培玉. 基于日志的安全审计系统研究与实现. 网络与信息安全，2009.4

[110] 王保云. 安全审计事件可视化关联分析技术研究. 解放军信息工程大学[硕士学位论文],2008.6
[111] 张惠玲,孙剑,邵海鹏. 基于贝叶斯推理的 HCM 延误模型修正. 计算机工程,2011.4
[112] 孙强. 信息系统审计：安全、风险管理与控制. 北京：机械工业出版社,2003
[113] 刘宝旭,马建民,池亚平. 计算机网络安全应急响应技术的分析与研究. 计算机工程,2007.5
[114] 吴晓平,付钰. 信息系统安全风险评估理论与方法. 北京：科学出版社,2011.
[115] 杨晓明,罗衡峰,范成瑜等. 信息系统安全风险评估技术分析. 计算机应用,2008.8
[116] 肖龙,戚湧,李千目. 基于 AHP 和模糊综合评判的信息安全风险评估. 计算机工程与应用,2009.8
[117] 陈鍊,文巨峰,韩冰青. 信息系统安全风险评估. 计算机工程与应用,2006.4
[118] 陈鍊,胡作进,蔡淑珍. 信息系统安全风险评估模型研究. 计算机应用与软件,2007.6
[119] 冯登国,孙锐,张阳. 信息安全体系结构. 北京：清华大学出版社,2008.9
[120] 施峰,胡昌振,刘炳华. 信息安全保密基础教程. 北京：北京理工大学出版社,2008.5
[121] 范红,胡志昂,金丽娜. 信息系统等级保护安全设计技术实现与使用. 北京：清华大学出版社,2010.6
[122] 许静，陈宏刚，王庆人. 软件测试方法简述与展望. 计算机工程与应用,2003.5
[123] 马瑞芳，王会燃. 计算机软件测试方法的研究. 小型微型计算机系统,2002.12